ΟΔΗΓΙΕΣ

ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 14ης Δεκεμβρίου 2022

σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2)

(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 Κεντρικής Τράπεζας ([1]),

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής ([2]),

Αφού ζήτησαν τη γνώμη της Επιτροπής των Περιφερειών,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία ([3]),

Εκτιμώντας τα ακόλουθα:

(1) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]) αποσκοπούσε στην ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, στον μετριασμό των απειλών για τα συστήματα δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών, ώστε να συμβάλει στην ασφάλεια και στην αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης.

(2) Μετά την έναρξη ισχύος της οδηγίας (ΕΕ) 2016/1148, έχει σημειωθεί σημαντική πρόοδος στην αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης. Η επανεξέταση της εν λόγω οδηγίας κατέδειξε ότι αυτή λειτούργησε ως καταλύτης για τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην Ένωση καθώς προετοίμασε το έδαφος για μια σημαντική αλλαγή νοοτροπίας. Με την οδηγία διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών με τη θέσπιση εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τη θέσπιση εθνικών ικανοτήτων και με την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και οντότητες που προσδιορίζονται από κάθε κράτος μέλος. Η οδηγία (ΕΕ) 2016/1148 συνέβαλε επίσης στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας συνεργασίας και του δικτύου εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών. Παρά τα επιτεύγματα αυτά, η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 αποκάλυψε εγγενείς αδυναμίες που την εμποδίζουν να αντιμετωπίσει αποτελεσματικά τις τρέχουσες και τις αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας.

(3) Τα συστήματα δικτύου και πληροφοριών έχουν εξελιχθεί σε κεντρικό στοιχείο της καθημερινής ζωής με τον ταχύ ψηφιακό μετασχηματισμό και τη διασύνδεση της κοινωνίας, μεταξύ άλλων στις διασυνοριακές ανταλλαγές. Η εξέλιξη αυτή έχει οδηγήσει σε επέκταση του τοπίου των κυβερνοαπειλών, γεγονός που δημιουργεί νέες προκλήσεις οι οποίες απαιτούν προσαρμοσμένες, συντονισμένες και καινοτόμες αποκρίσεις σε όλα τα κράτη μέλη. Ο αριθμός, το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Ως εκ τούτου, τα περιστατικά μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων στην εσωτερική αγορά, να προκαλέσουν οικονομικές απώλειες, να υπονομεύσουν την

([1]) ΕΕ C 233 της 16.6.2022, σ. 22.
([2]) ΕΕ C 286 της 16.7.2021, σ. 170.
([3]) Θέση του Ευρωπαϊκού Κοινοβουλίου της 10ης Νοεμβρίου 2022 (δεν έχει ακόμη δημοσιευθεί στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 28ης Νοεμβρίου 2022.
([4]) 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).

εμπιστοσύνη των χρηστών και να προκαλέσουν σοβαρή ζημία στην οικονομία και την κοινωνία της Ένωσης. Ως εκ τούτου, η ετοιμότητα και η αποτελεσματικότητα στον τομέα της κυβερνοασφάλειας είναι πλέον πιο σημαντικές από ποτέ για την ορθή λειτουργία της εσωτερικής αγοράς. Επιπλέον, σε πολλούς κρίσιμους τομείς η κυβερνοασφάλεια αποτελεί βασικό παράγοντα για την αποδοχή του ψηφιακού μετασχηματισμού και την πλήρη αξιοποίηση των οικονομικών, κοινωνικών και βιώσιμων οφελών της ψηφιοποίησης.

(4) Η νομική βάση της οδηγίας (ΕΕ) 2016/1148 ήταν το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για την προσέγγιση των εθνικών κανόνων. Οι απαιτήσεις κυβερνοασφάλειας που επιβάλλονται στις οντότητες που παρέχουν υπηρεσίες ή ασκούν οικονομικά σημαντικές δραστηριότητες ποικίλλουν σημαντικά μεταξύ των κρατών μελών ως προς το είδος των απαιτήσεων, τον βαθμό λεπτομέρειάς τους και τη μέθοδο εποπτείας. Οι διαφορές αυτές συνεπάγονται πρόσθετο κόστος και προκαλούν δυσκολίες στις οντότητες που προσφέρουν αγαθά ή υπηρεσίες διασυνοριακά. Απαιτήσεις που επιβάλλονται από ένα κράτος μέλος και οι οποίες διαφέρουν, ή ακόμη και έρχονται σε αντίθεση με αυτές που επιβάλλει άλλο κράτος μέλος, ενδέχεται να επηρεάσουν σημαντικά τις εν λόγω διασυνοριακές δραστηριότητες. Επιπλέον, η πιθανότητα ανεπαρκούς σχεδιασμού ή εφαρμογής των απαιτήσεων κυβερνοασφάλειας σε ένα κράτος μέλος είναι πιθανό να έχει επιπτώσεις στο επίπεδο κυβερνοασφάλειας άλλων κρατών μελών, ιδίως δεδομένης της έντασης των διασυνοριακών ανταλλαγών. Η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 κατέδειξε μεγάλη απόκλιση στην εφαρμογή της από τα κράτη μέλη, μεταξύ άλλων όσον αφορά το πεδίο εφαρμογής της, η οριοθέτηση του οποίου επαφίεται σε μεγάλο βαθμό στη διακριτική ευχέρεια των κρατών μελών. Η οδηγία (ΕΕ) 2016/1148 παρείχε επίσης ευρύτατη διακριτική ευχέρεια στα κράτη μέλη όσον αφορά την εφαρμογή των υποχρεώσεων σχετικά με την ασφάλεια και την αναφορά των περιστατικών που ορίζονται στην εν λόγω οδηγία. Ως εκ τούτου, οι υποχρεώσεις αυτές εκπληρώθηκαν με πολύ διαφορετικούς τρόπους σε εθνικό επίπεδο. Παρόμοιες αποκλίσεις υπάρχουν στην εφαρμογή των διατάξεων της οδηγίας (ΕΕ) 2016/1148 για την εποπτεία και την επιβολή.

(5) Όλες αυτές οι αποκλίσεις έχουν ως αποτέλεσμα τον κατακερματισμό της εσωτερικής αγοράς και ενδέχεται να έχουν αρνητικές επιπτώσεις στη λειτουργία της, επηρεάζοντας ιδίως τη διασυνοριακή παροχή υπηρεσιών και το επίπεδο κυβερνοανθεκτικότητας λόγω της εφαρμογής πολλαπλών μέτρων. Εντέλει, οι αποκλίσεις αυτές θα μπορούσαν να οδηγήσουν στη μεγαλύτερη ευπάθεια ορισμένων κρατών μελών έναντι κυβερνοαπειλών, με δυνητικές δευτερογενείς επιπτώσεις σε ολόκληρη την Ένωση. Η παρούσα οδηγία αποσκοπεί στην εξάλειψη αυτών των μεγάλων αποκλίσεων μεταξύ των κρατών μελών, ιδίως με τον καθορισμό ελάχιστων κανόνων σχετικά με τη λειτουργία ενός συντονισμένου κανονιστικού πλαισίου, με τη θέσπιση μηχανισμών για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος, με την επικαιροποίηση του καταλόγου των τομέων και δραστηριοτήτων που υπόκεινται σε υποχρεώσεις κυβερνοασφάλειας και με τη θέσπιση αποτελεσματικών ένδικων μέσων και μέτρων επιβολής που έχουν καθοριστική σημασία για την αποτελεσματική επιβολή των εν λόγω υποχρεώσεων. Ως εκ τούτου, η οδηγία (ΕΕ) 2016/1148 θα πρέπει να καταργηθεί και να αντικατασταθεί από την παρούσα οδηγία.

(6) Με την κατάργηση της οδηγίας (ΕΕ) 2016/1148, το πεδίο εφαρμογής ανά τομείς θα πρέπει να επεκταθεί σε μεγαλύτερο μέρος της οικονομίας για να παρέχεται ολοκληρωμένη κάλυψη των τομέων και υπηρεσιών ζωτικής σημασίας για βασικές κοινωνιακές και οικονομικές δραστηριότητες στην εσωτερική αγορά. Ειδικότερα, η παρούσα οδηγία αποσκοπεί στην αντιμετώπιση των ελλείψεων λόγω της διαφοροποίησης μεταξύ των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών, η οποία έχει αποδειχθεί παρωχημένη, δεδομένου ότι δεν αποτυπώνει τη σημασία των τομέων ή των υπηρεσιών για τις κοινωνικές και οικονομικές δραστηριότητες στην εσωτερική αγορά.

(7) Σύμφωνα με την οδηγία (ΕΕ) 2016/1148, τα κράτη μέλη έφεραν την ευθύνη του προσδιορισμού των οντοτήτων που πληρούν τα κριτήρια του ορισμού του φορέα εκμετάλλευσης βασικών υπηρεσιών. Προκειμένου να εξαλειφθούν οι μεγάλες αποκλίσεις μεταξύ των κρατών μελών ως προς το θέμα αυτό και να διασφαλιστεί για όλες τις σχετικές οντότητες ασφάλεια δικαίου όσον αφορά τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών, θα πρέπει να θεσπιστεί ενιαίο κριτήριο για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Το κριτήριο αυτό θα πρέπει να συνίσταται στην εφαρμογή ενός κανόνα ανώτατου ορίου μεγέθους, σύμφωνα με τον οποίο όλες οι οντότητες που χαρακτηρίζονται μεσαίες επιχειρήσεις δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ της Επιτροπής ([5]) ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις

([5]) Σύσταση 2003/361/ΕΚ 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).

που προβλέπονται στην παράγραφο 1 του εν λόγω άρθρου και που δραστηριοποιούνται στους τομείς και παρέχουν τα είδη υπηρεσιών ή ασκούν τις δραστηριότητες που καλύπτονται από την παρούσα οδηγία εμπίπτουν στο πεδίο εφαρμογής του. Τα κράτη μέλη θα πρέπει επίσης να προβλέπουν ότι ορισμένες μικρές επιχειρήσεις και πολύ μικρές επιχειρήσεις, όπως καθορίζονται στο άρθρο 2 παράγραφοι 2 και 3 του εν λόγω παραρτήματος, που πληρούν ειδικά κριτήρια τα οποία υποδεικνύουν βασικό ρόλο για την κοινωνία, την οικονομία ή για συγκεκριμένους τομείς ή τύπους υπηρεσιών εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(8) Η εξαίρεση των οντοτήτων δημόσιας διοίκησης από το πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να εφαρμόζεται σε οντότητες των οποίων οι δραστηριότητες εντάσσονται κατά κύριο λόγο στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένης της πρόληψης, της διερεύνησης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων. Ωστόσο, οι οντότητες δημόσιας διοίκησης των οποίων οι δραστηριότητες συνδέονται μόνο οριακά με τους εν λόγω τομείς δεν θα πρέπει να εξαιρεθούν από το πεδίο εφαρμογής της παρούσας οδηγίας. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες με ρυθμιστικές αρμοδιότητες δεν θεωρείται ότι ασκούν δραστηριότητες στον τομέα της επιβολής του νόμου και, επομένως, δεν εξαιρούνται για τον λόγο αυτό από το πεδίο εφαρμογής της παρούσας οδηγίας. Οι φορείς δημόσιας διοίκησης που ιδρύονται από κοινού με τρίτη χώρα σύμφωνα με διεθνή συμφωνία εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας. Η παρούσα οδηγία δεν εφαρμόζεται στις διπλωματικές και προξενικές αποστολές κρατών μελών σε τρίτες χώρες ή στα συστήματα δικτύου και πληροφοριών τους, όταν τα συστήματα αυτά βρίσκονται στις εγκαταστάσεις της αποστολής ή λειτουργούν για χρήστες σε τρίτη χώρα.

(9) Τα κράτη μέλη θα πρέπει να είναι σε θέση να λαμβάνουν τα αναγκαία μέτρα για την προστασία των ουσιωδών συμφερόντων εθνικής ασφάλειας, τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να μπορούν να εξαιρούν συγκεκριμένες οντότητες που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένων και των δραστηριοτήτων που σχετίζονται με την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων, από ορισμένες υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά τις εν λόγω δραστηριότητες. Όταν μια οντότητα παρέχει υπηρεσίες αποκλειστικά σε οντότητα δημόσιας διοίκησης που εξαιρείται από το πεδίο εφαρμογής της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να μπορούν να αποφασίζουν ότι η εν λόγω οντότητα εξαιρείται από τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά τις εν λόγω υπηρεσίες. Επιπλέον, σύμφωνα με το άρθρο 346 ΣΛΕΕ, κανένα κράτος μέλος δεν θα πρέπει να υποχρεούται να παρέχει πληροφορίες, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς ουσιώδη συμφέροντα της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της άμυνάς του. Στο πλαίσιο αυτό, οι εθνικοί και ενωσιακοί κανόνες για την προστασία διαβαθμισμένων πληροφοριών, οι συμφωνίες εμπιστευτικότητας και οι άτυπες συμφωνίες εμπιστευτικότητας, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light Protocol», θα πρέπει να λαμβάνονται υπόψη. Το πρωτόκολλο για την ανταλλαγή πληροφοριών πρέπει να νοείται ως μέσο που επιτρέπει την παροχή πληροφοριών σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση των πληροφοριών. Χρησιμοποιείται σε όλες σχεδόν τις ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT) και σε ορισμένα κέντρα ανάλυσης και ανταλλαγής πληροφοριών.

(10) Μολονότι η παρούσα οδηγία εφαρμόζεται σε οντότητες που ασκούν δραστηριότητες στον τομέα της παραγωγής ηλεκτρικής ενέργειας από πυρηνικούς σταθμούς, ορισμένες από τις εν λόγω δραστηριότητες μπορεί να συνδέονται με την εθνική ασφάλεια. Στην περίπτωση αυτή, τα κράτη μέλη θα πρέπει να είναι σε θέση να ασκούν την αρμοδιότητά τους για τη διαφύλαξη της εθνικής ασφάλειας όσον αφορά τις εν λόγω δραστηριότητες, συμπεριλαμβανομένων των δραστηριοτήτων εντός της αλυσίδας αξίας της πυρηνικής ενέργειας, σύμφωνα με τις Συνθήκες.

(11) Ορισμένες οντότητες ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένης της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων, παρέχοντας παράλληλα υπηρεσίες εμπιστοσύνης. Οι πάροχοι υπηρεσιών εμπιστοσύνης που υπάγονται στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) θα πρέπει να υπάγονται στο πεδίο εφαρμογής της παρούσας οδηγίας, προκειμένου να διασφαλίζεται το ίδιο επίπεδο απαιτήσεων ασφάλειας και εποπτείας με εκείνο που προβλεπόταν προηγουμένως στον εν λόγω κανονισμό σε σχέση με τους παρόχους υπηρεσιών εμπιστοσύνης. Σύμφωνα με την εξαίρεση κάποιων ορισμένων από τον κανονισμό (ΕΕ) αριθ. 910/2014 ειδικών υπηρεσιών, η παρούσα οδηγία δεν θα πρέπει να εφαρμόζεται στην παροχή υπηρεσιών εμπιστοσύνης που χρησιμοποιούνται αποκλειστικά στο πλαίσιο κλειστών συστημάτων που απορρέουν από το εθνικό δίκαιο ή από συμφωνίες μεταξύ καθορισμένου συνόλου συμμετεχόντων.

([6]) 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).

(12) Οι φορείς παροχής ταχυδρομικών υπηρεσιών κατά την έννοια της οδηγίας 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), συμπεριλαμβανομένων των παρόχων υπηρεσιών ταχυμεταφοράς, θα πρέπει να εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας εάν παρέχουν τουλάχιστον ένα από τα στάδια της αλυσίδας ταχυδρομικής διανομής, και ιδίως την περισυλλογή, τη διαλογή, τη μεταφορά ή τη διανομή ταχυδρομικών αντικειμένων, συμπεριλαμβανομένων των υπηρεσιών παραλαβής, λαμβάνοντας παράλληλα υπόψη τον βαθμό εξάρτησής τους από τα συστήματα δικτύου και πληροφοριών. Οι υπηρεσίες μεταφορών που δεν πραγματοποιούνται σε συνδυασμό με ένα από τα στάδια αυτά θα πρέπει να εξαιρούνται από το πεδίο των ταχυδρομικών υπηρεσιών.

(13) Δεδομένης της εντατικοποίησης και της αυξημένης πολυπλοκότητας των κυβερνοαπειλών, τα κράτη μέλη θα πρέπει να επιδιώξουν να διασφαλίσουν ότι οι οντότητες που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας επιτυγχάνουν υψηλό επίπεδο κυβερνοασφάλειας και να στηρίξουν την εφαρμογή ισοδύναμων μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που αντικατοπτρίζουν τον ευαίσθητο χαρακτήρα των εν λόγω οντοτήτων.

(14) Το δίκαιο της Ένωσης για την προστασία των δεδομένων και το δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας εφαρμόζονται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει της παρούσας οδηγίας. Συγκεκριμένα, η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) και της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]). Κατά συνέπεια, η παρούσα οδηγία δεν θα πρέπει να θίγει, μεταξύ άλλων, τα καθήκοντα και τις εξουσίες των αρχών που είναι αρμόδιες για την παρακολούθηση της συμμόρφωσης με το ισχύον ενωσιακό δίκαιο για την προστασία των δεδομένων και το ενωσιακό δίκαιο για την προστασία της ιδιωτικότητας.

(15) Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας για τους σκοπούς της συμμόρφωσης με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις υποβολής αναφορών θα πρέπει να ταξινομούνται σε δύο κατηγορίες, σε βασικές οντότητες και σημαντικές οντότητες, ώστε να αντικατοπτρίζονται ο βαθμός κρισιμότητάς τους, όσον αφορά τον τομέα τους ή το είδος της υπηρεσίας που παρέχουν, καθώς και το μέγεθός τους. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνονται δεόντως υπόψη τυχόν σχετικές τομεακές εκτιμήσεις κινδύνου ή καθοδήγηση από τις αρμόδιες αρχές, κατά περίπτωση. Τα καθεστώτα εποπτείας και επιβολής για τις δύο αυτές κατηγορίες οντοτήτων θα πρέπει να διαφοροποιούνται ώστε να εξασφαλίζεται δίκαιη ισορροπία μεταξύ των απαιτήσεων και των υποχρεώσεων με βάση τον κίνδυνο, αφενός, και του διοικητικού φόρτου που προκύπτει από την εποπτεία της συμμόρφωσης, αφετέρου.

(16) Προκειμένου να αποφευχθεί το ενδεχόμενο, οντότητες που έχουν συνεργαζόμενες επιχειρήσεις ή είναι συνδεδεμένες επιχειρήσεις να θεωρούνται βασικές ή σημαντικές οντότητες όταν αυτό θα ήταν δυσανάλογο, τα κράτη μέλη μπορούν να λαμβάνουν υπόψη τον βαθμό ανεξαρτησίας που έχει μια οντότητα σε σχέση με τον εταίρο της ή τις συνδεδεμένες επιχειρήσεις, κατά την εφαρμογή του άρθρου 6 παράγραφος 2 του παραρτήματος της σύστασης 2003/361/ΕΚ. Πιο συγκεκριμένα, τα κράτη μέλη μπορούν να λαμβάνουν υπόψη το γεγονός ότι μια οντότητα είναι ανεξάρτητη από τον εταίρο της ή τις συνδεδεμένες επιχειρήσεις όσον αφορά τα συστήματα δικτύου και πληροφοριών που χρησιμοποιεί η εν λόγω οντότητα για την παροχή των υπηρεσιών της και όσον αφορά τις υπηρεσίες που παρέχει η οντότητα. Σε αυτή τη βάση, κατά περίπτωση, τα κράτη μέλη μπορούν να θεωρούν ότι μια τέτοια οντότητα δεν συνιστά μεσαία επιχείρηση δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ, ή δεν υπερβαίνει τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στην παράγραφο 1 του εν λόγω άρθρου, εάν, αφού ληφθεί υπόψη ο βαθμός ανεξαρτησίας της εν λόγω οντότητας, η εν λόγω οντότητα δεν θα είχε θεωρηθεί ως μεσαία επιχείρηση ή ότι υπερβαίνει τα εν λόγω ανώτατα όρια σε περίπτωση που είχαν ληφθεί υπόψη μόνο τα δικά της δεδομένα. Αυτό δεν θίγει τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία για τις συνεργαζόμενες και τις συνδεδεμένες επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(17) Τα κράτη μέλη θα πρέπει να είναι σε θέση να αποφασίσουν εάν οι οντότητες που προσδιορίστηκαν πριν από την έναρξη ισχύος της παρούσας οδηγίας ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148, πρέπει να θεωρούνται βασικές οντότητες.

([7]) Οδηγία 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Δεκεμβρίου 1997, σχετικά με τους κοινούς κανόνες για την ανάπτυξη της εσωτερικής αγοράς κοινοτικών ταχυδρομικών υπηρεσιών και τη βελτίωση της ποιότητας των παρεχομένων υπηρεσιών (ΕΕ L 15 της 21.1.1998, σ. 14).

([8]) 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).

([9]) 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 της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

(18) Προκειμένου να διασφαλιστεί σαφής επισκόπηση των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να καταρτίσουν κατάλογο βασικών και σημαντικών οντοτήτων καθώς και οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να απαιτούν από τις οντότητες να υποβάλλουν στις αρμόδιες αρχές τουλάχιστον τις ακόλουθες πληροφορίες, συγκεκριμένα το όνομα, τη διεύθυνση και τα επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου, των πεδίων IP και των αριθμών τηλεφώνου της οντότητας, και κατά περίπτωση, του σχετικού τομέα και υποτομέα που αναφέρονται στα παραρτήματα, καθώς και, κατά περίπτωση, κατάλογο των κρατών μελών στα οποία παρέχουν υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Για τον σκοπό αυτό, η Επιτροπή, με τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), θα πρέπει, χωρίς αδικαιολόγητη καθυστέρηση, να προβλέπει κατευθυντήριες γραμμές και υποδείγματα σχετικά με την υποχρέωση υποβολής πληροφοριών. Για να διευκολυνθεί η κατάρτιση και η επικαιροποίηση του καταλόγου των βασικών και σημαντικών οντοτήτων καθώς και των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, τα κράτη μέλη θα πρέπει να είναι σε θέση να θεσπίζουν εθνικούς μηχανισμούς για την εγγραφή των οντοτήτων αυτών. Όταν υπάρχουν μητρώα σε εθνικό επίπεδο, τα κράτη μέλη μπορούν να αποφασίζουν σχετικά με τους κατάλληλους μηχανισμούς που επιτρέπουν τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

(19) Τα κράτη μέλη θα πρέπει να φέρουν την ευθύνη για την υποβολή στην Επιτροπή τουλάχιστον του αριθμού των βασικών και σημαντικών οντοτήτων για κάθε τομέα και υποτομέα που αναφέρεται στα παραρτήματα, καθώς και των πληροφοριών σχετικά με τον αριθμό των προσδιορισμένων οντοτήτων και τη διάταξη της παρούσας οδηγίας, βάσει της οποίας ορίστηκαν ως τέτοιες, και το είδος της υπηρεσίας που παρέχουν. Τα κράτη μέλη ενθαρρύνονται να ανταλλάσσουν με την Επιτροπή πληροφορίες σχετικά με βασικές και σημαντικές οντότητες και, σε περίπτωση περιστατικού μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, σχετικές πληροφορίες όπως το όνομα της οικείας οντότητας.

(20) Η Επιτροπή θα πρέπει, σε συνεργασία με την Ομάδα Συνεργασίας και κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, να προβλέπει κατευθυντήριες γραμμές σχετικά με την εφαρμογή των κριτηρίων που ισχύουν για τις πολύ μικρές και τις μικρές επιχειρήσεις προκειμένου να αξιολογήσει εάν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Η Επιτροπή θα πρέπει επίσης να διασφαλίσει ότι παρέχεται κατάλληλη καθοδήγηση στις πολύ μικρές και μικρές επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας. Η Επιτροπή θα πρέπει, με τη βοήθεια των κρατών μελών, να θέτει σχετικές πληροφορίες στη διάθεση των πολύ μικρών και των μικρών επιχειρήσεων.

(21) Η Επιτροπή θα μπορούσε να παρέχει καθοδήγηση για να βοηθά τα κράτη μέλη στην εφαρμογή των διατάξεων της παρούσας οδηγίας σχετικά με το πεδίο εφαρμογής και την αξιολόγηση της αναλογικότητας των μέτρων που πρέπει να ληφθούν δυνάμει της παρούσας οδηγίας, ιδίως όσον αφορά οντότητες με σύνθετα επιχειρηματικά μοντέλα ή περιβάλλοντα λειτουργίας, σε περιπτώσεις όπου μια οντότητα μπορεί να πληροί ταυτόχρονα τα κριτήρια που αντιστοιχούν τόσο σε βασικές όσο και σε σημαντικές οντότητες ή να ασκεί ταυτόχρονα δραστηριότητες, ορισμένες από τις οποίες εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας και ορισμένες από τις οποίες εξαιρούνται από το πεδίο εφαρμογής της.

(22) Η παρούσα οδηγία καθορίζει τη βάση αναφοράς για τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών σε όλους τους τομείς που εμπίπτουν στο πεδίο εφαρμογής της. Προκειμένου να αποφευχθεί ο κατακερματισμός των διατάξεων περί κυβερνοασφάλειας των νομικών πράξεων της Ένωσης, όταν περαιτέρω τομεακές νομικές πράξεις της Ένωσης που αφορούν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις υποβολής εκθέσεων θεωρούνται αναγκαίες για τη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, η Επιτροπή θα πρέπει να αξιολογήσει κατά πόσον οι εν λόγω επιπλέον διατάξεις θα μπορούσαν να καθοριστούν σε εκτελεστική πράξη δυνάμει της παρούσας οδηγίας. Εάν οι εκτελεστική πράξη δεν είναι κατάλληλη για τον σκοπό αυτό, οι τομεακές νομικές πράξεις της Ένωσης θα μπορούσαν να συμβάλουν στη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, λαμβάνοντας παράλληλα πλήρως υπόψη τις ιδιαιτερότητες και την πολυπλοκότητα των σχετικών τομέων. Για τον σκοπό αυτό, η παρούσα οδηγία δεν αποκλείει την έκδοση περαιτέρω τομεακών νομικών πράξεων της Ένωσης για την αντιμετώπιση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων κοινοποίησης περιστατικών που λαμβάνουν δεόντως υπόψη την ανάγκη για ένα ολοκληρωμένο και συνεκτικό πλαίσιο κυβερνοασφάλειας. Η παρούσα οδηγία δεν θίγει τις υφιστάμενες εκτελεστικές αρμοδιότητες που έχουν ανατεθεί στην Επιτροπή σε διάφορους τομείς, συμπεριλαμβανομένων των μεταφορών και της ενέργειας.

(23) Όταν μια τομεακή νομική πράξη της Ένωσης περιέχει διατάξεις που απαιτούν από βασικές ή σημαντικές οντότητες να εγκρίνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή να κοινοποιούν σημαντικά περιστατικά, και όταν οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην

παρούσα οδηγία, οι εν λόγω διατάξεις, μεταξύ άλλων σχετικά με την εποπτεία και την επιβολή, θα πρέπει να εφαρμόζονται στις εν λόγω οντότητες. Εάν μια τομεακή νομική πράξη της Ένωσης δεν καλύπτει όλες τις οντότητες σε συγκεκριμένο τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας θα πρέπει να εξακολουθήσουν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από την εν λόγω πράξη.

(24) Όταν οι διατάξεις τομεακής νομικής πράξης της Ένωσης απαιτούν από βασικές ή σημαντικές οντότητες να συμμορφωθούν με υποχρεώσεις κοινοποίησης που είναι τουλάχιστον ισοδύναμου αποτελέσματος με τις υποχρεώσεις κοινοποίησης που ορίζονται στην παρούσα οδηγία, θα πρέπει να διασφαλίζεται η συνοχή και η αποτελεσματικότητα του χειρισμού των κοινοποιήσεων περιστατικών. Για τον σκοπό αυτό, οι διατάξεις της τομεακής νομικής πράξης της Ένωσης για την κοινοποίηση περιστατικών θα πρέπει να παρέχουν στις CSIRT, στις αρμόδιες αρχές ή στα ενιαία σημεία επαφής για την κυβερνοασφάλεια (ενιαία σημεία επαφής) δυνάμει της παρούσας οδηγίας άμεση πρόσβαση στις κοινοποιήσεις περιστατικών που υποβάλλονται σύμφωνα με την τομεακή νομική πράξη της Ένωσης. Ειδικότερα, η εν λόγω άμεση πρόσβαση μπορεί να διασφαλιστεί εάν οι κοινοποιήσεις περιστατικών διαβιβάζονται αμελλητί στην CSIRT, στην αρμόδια αρχή ή στο ενιαίο σημείο επαφής δυνάμει της παρούσας οδηγίας. Κατά περίπτωση, τα κράτη μέλη θα πρέπει να θεσπίσουν μηχανισμό αυτόματης και άμεσης αναφοράς που να διασφαλίζει τη συστηματική και άμεση ανταλλαγή πληροφοριών με τις CSIRT, τις αρμόδιες αρχές ή το ενιαίο σημείο επαφής σχετικά με τον χειρισμό των εν λόγω κοινοποιήσεων περιστατικών. Για τους σκοπούς της απλούστευσης της κοινοποίησης και της εφαρμογής του μηχανισμού αυτόματης και άμεσης υποβολής αναφορών, τα κράτη μέλη θα μπορούσαν, σύμφωνα με την τομεακή νομική πράξη της Ένωσης, να χρησιμοποιούν ενιαίο σημείο εισόδου.

(25) Οι τομεακές νομικές πράξεις της Ένωσης που προβλέπουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή υποχρεώσεις υποβολής εκθέσεων τουλάχιστον ισοδύναμου αποτελέσματος με εκείνες που ορίζονται στην παρούσα οδηγία, θα μπορούσαν να προβλέπουν ότι οι αρμόδιες αρχές δυνάμει των εν λόγω πράξεων ασκούν τις εποπτικές και εκτελεστικές αρμοδιότητές τους σε σχέση με τα εν λόγω μέτρα ή υποχρεώσεις με τη συνδρομή των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας. Οι οικείες αρμόδιες αρχές θα μπορούσαν να προβούν σε ρυθμίσεις συνεργασίας για τον σκοπό αυτό. Οι εν λόγω ρυθμίσεις συνεργασίας θα μπορούσαν να προσδιορίζουν, μεταξύ άλλων, τις διαδικασίες που αφορούν τον συντονισμό των εποπτικών δραστηριοτήτων, συμπεριλαμβανομένων των διαδικασιών των ερευνών και των επιτόπιων επιθεωρήσεων σύμφωνα με το εθνικό δίκαιο και ενός μηχανισμού για την ανταλλαγή σχετικών πληροφοριών, σχετικά με την εποπτεία και την επιβολή μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της πρόσβασης σε σχετικές με τον κυβερνοχώρο πληροφορίες που ζητούν οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας.

(26) Όταν ειδικές τομεακές νομικές πράξεις της Ένωσης απαιτούν ή παρέχουν κίνητρα σε οντότητες για την κοινοποίηση σημαντικών κυβερνοαπειλών, τα κράτη μέλη θα πρέπει επίσης να ενθαρρύνουν την ανταλλαγή σημαντικών κυβερνοαπειλών με τις CSIRT, τις αρμόδιες αρχές ή τα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας, προκειμένου να διασφαλίζεται ενισχυμένο επίπεδο ευαισθητοποίησης των εν λόγω οργάνων σχετικά με το τοπίο των κυβερνοαπειλών και να τους παρέχεται η δυνατότητα να ανταποκρίνονται αποτελεσματικά και εγκαίρως σε περίπτωση επέλευσης των σημαντικών κυβερνοαπειλών.

(27) Οι μελλοντικές τομεακές νομικές πράξεις της Ένωσης θα πρέπει να λαμβάνουν δεόντως υπόψη τους ορισμούς και το πλαίσιο εποπτείας και επιβολής που καθορίζονται στην παρούσα οδηγία.

(28) Ο κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]) θα πρέπει να θεωρείται τομεακή νομική πράξη της Ένωσης σε σχέση με την παρούσα οδηγία όσον αφορά τις οντότητες του χρηματοπιστωτικού τομέα. Αντί των διατάξεων που θεσπίζονται στην παρούσα οδηγία, θα πρέπει να εφαρμόζονται οι διατάξεις του κανονισμού (ΕΕ) 2022/2554 σχετικά με τη διαχείριση κινδύνων της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), τη διαχείριση περιστατικών που σχετίζονται με τις ΤΠΕ και ιδίως την αναφορά σοβαρών περιστατικών ΤΠΕ, καθώς και σχετικά με τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, τις ρυθμίσεις ανταλλαγής πληροφοριών και τον κίνδυνο τρίτων παρόχων ΤΠΕ. Ως εκ τούτου, τα κράτη μέλη δεν θα πρέπει να εφαρμόζουν τις διατάξεις της παρούσας οδηγίας σχετικά με τις υποχρεώσεις διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και αναφοράς περιστατικών και την εποπτεία, καθώς και την επιβολή της νομοθεσίας στις χρηματοπιστωτικές οντότητες που καλύπτονται από τον κανονισμό (ΕΕ) 2022/2554. Ταυτόχρονα, είναι σημαντικό να διατηρηθεί στενή σχέση και ανταλλαγή πληροφοριών με τον χρηματοπιστωτικό τομέα στο πλαίσιο της παρούσας οδηγίας. Για τον σκοπό αυτό, ο κανονισμός (ΕΕ) 2022/2554 επιτρέπει στις Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και στις αρμόδιες αρχές δυνάμει του εν λόγω κανονισμού να συμμετέχουν στις δραστηριότητες της Ομάδας Συνεργασίας και να ανταλλάσσουν πληροφορίες και να συνεργάζονται με τα ενιαία σημεία επαφής, καθώς και με τις CSIRT και τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας. Οι αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554 θα

([10]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (βλέπε σελίδα 1 της παρούσας Επίσημης Εφημερίδας).

πρέπει επίσης να διαβιβάζουν λεπτομερή στοιχεία για σημαντικά περιστατικά που σχετίζονται με τις ΤΠΕ και, κατά περίπτωση, σημαντικές κυβερνοαπειλές στις CSIRT, στις αρμόδιες αρχές ή στα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας. Αυτό μπορεί να επιτευχθεί με την παροχή άμεσης πρόσβασης στην κοινοποίηση των περιστατικών και την διαβίβασή τους απευθείας ή μέσω ενός ενιαίου σημείου εισόδου. Επιπλέον, τα κράτη μέλη θα πρέπει να συνεχίσουν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις στρατηγικές τους για την κυβερνοασφάλεια, και οι CSIRT μπορούν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις δραστηριότητές τους.

(29) Προκειμένου να αποφευχθούν κενά ή αλληλεπικαλύψεις των υποχρεώσεων κυβερνοασφάλειας που επιβάλλονται σε οντότητες στον τομέα των αερομεταφορών, οι εθνικές αρχές δυνάμει των κανονισμών (ΕΚ) αριθ. 300/2008 ([11]) και (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]) και οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας θα πρέπει να συνεργάζονται σε σχέση με την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και την εποπτεία της συμμόρφωσης με τα εν λόγω μέτρα σε εθνικό επίπεδο. Η συμμόρφωση μιας οντότητας με τις απαιτήσεις ασφάλειας που καθορίζονται στους κανονισμούς (ΕΚ) αριθ. 300/2008 και (ΕΕ) 2018/1139 και στις σχετικές κατ' εξουσιοδότηση και εκτελεστικές πράξεις που εκδίδονται σύμφωνα με τους εν λόγω κανονισμούς θα μπορούσε να θεωρηθεί από τις αρμόδιες αρχές βάσει της παρούσας οδηγίας ότι συνιστά συμμόρφωση με τις αντίστοιχες απαιτήσεις που καθορίζονται στην παρούσα οδηγία.

(30) Λαμβανομένων υπόψη των διασυνδέσεων μεταξύ της κυβερνοασφάλειας και της φυσικής ασφάλειας των οντοτήτων, θα πρέπει να διασφαλιστεί μια συνεκτική προσέγγιση μεταξύ της οδηγίας (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]) και της παρούσας οδηγίας. Για να επιτευχθεί αυτό, οι οντότητες που χαρακτηρίζονται ως κρίσιμες οντότητες σύμφωνα με την οδηγία (ΕΕ) 2022/2557 θα πρέπει να θεωρούνται βασικές οντότητες δυνάμει της παρούσας οδηγίας. Επιπλέον, κάθε κράτος μέλος θα πρέπει να διασφαλίζει ότι η εθνική στρατηγική του για την κυβερνοασφάλεια προβλέπει ένα πλαίσιο πολιτικής για ενισχυμένο συντονισμό εντός του εν λόγω κράτους μέλους μεταξύ των αρμόδιων αρχών του δυνάμει της παρούσας οδηγίας και των αρχών που προβλέπονται στην οδηγία (ΕΕ) 2022/2557, στο πλαίσιο της ανταλλαγής πληροφοριών σχετικά με κινδύνους, απειλές και περιστατικά στον κυβερνοχώρο, καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός κυβερνοχώρου, και την άσκηση εποπτικών καθηκόντων. Οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες αμελλητί, ιδίως όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, των κινδύνων, των κυβερνοαπειλών και των περιστατικών, καθώς και σε σχέση με κινδύνους, απειλές και περιστατικά μη σχετιζόμενα με τον κυβερνοχώρο, που επηρεάζουν κρίσιμες οντότητες, συμπεριλαμβανομένων των μέτρων κυβερνοασφάλειας και των φυσικών μέτρων που λαμβάνονται από κρίσιμες οντότητες, καθώς και των αποτελεσμάτων των εποπτικών δραστηριοτήτων που διεξάγονται σε σχέση με τις εν λόγω οντότητες.

Επιπλέον, προκειμένου να εξορθολογιστούν οι εποπτικές δραστηριότητες μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και των αρμοδίων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2557 και προκειμένου να ελαχιστοποιηθεί ο διοικητικός φόρτος για τις οικείες οντότητες, οι εν λόγω αρμόδιες αρχές θα πρέπει να προσπαθήσουν να εναρμονίσουν τα υποδείγματα κοινοποίησης περιστατικών και τις εποπτικές διαδικασίες. Κατά περίπτωση, οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557, θα πρέπει να μπορούν να ζητούν από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας να ασκούν τις εποπτικές και εκτελεστικές αρμοδιότητές τους σε σχέση με οντότητα η οποία προσδιορίζεται ως κρίσιμη οντότητα βάσει της οδηγίας (ΕΕ) 2022/2557. Οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει, ει δυνατόν σε πραγματικό χρόνο, να συνεργάζονται και να ανταλλάσσουν πληροφορίες για τον σκοπό αυτό.

(31) Οι οντότητες που ανήκουν στον τομέα των ψηφιακών υποδομών στηρίζονται επί της ουσίας σε συστήματα δικτύου και πληροφοριών και, επομένως, οι υποχρεώσεις που επιβάλλονται σε αυτές σύμφωνα με την παρούσα οδηγία θα πρέπει να διαχειριστούν με ολοκληρωμένο τρόπο τη φυσική ασφάλεια των εν λόγω συστημάτων στο πλαίσιο των υποχρεώσεών τους όσον αφορά τη λήψη μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και την κοινοποίηση περιστατικών. Δεδομένου ότι τα θέματα αυτά καλύπτονται από την παρούσα οδηγία, οι υποχρεώσεις που προβλέπονται στα κεφάλαια III, IV και VI της οδηγίας (ΕΕ) 2022/2557 δεν ισχύουν για τις εν λόγω οντότητες.

([11]) Κανονισμός (ΕΚ) αριθ. 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2008, για τη θέσπιση κοινών κανόνων στο πεδίο της ασφάλειας της πολιτικής αεροπορίας και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2320/2002 (ΕΕ L 97 της 9.4.2008, σ. 72).

([12]) Κανονισμός (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2018, για τη θέσπιση κοινών κανόνων στον τομέα της πολιτικής αεροπορίας και την ίδρυση Οργανισμού της Ευρωπαϊκής Ένωσης για την Αεροπορική Ασφάλεια, και για την τροποποίηση των κανονισμών (ΕΚ) αριθ. 2111/2005, (ΕΚ) αριθ. 1008/2008, (ΕΕ) αριθ. 996/2010, (ΕΕ) αριθ. 376/2014 και των οδηγιών 2014/30/ΕΕ και 2014/53/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και για την κατάργηση των κανονισμών (ΕΚ) αριθ. 552/2004 και (ΕΚ) αριθ. 216/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΟΚ) αριθ. 3922/91 του Συμβουλίου (ΕΕ L 212 της 22.8.2018, σ. 1).

([13]) Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (βλέπε σελίδα 164 της παρούσας Επίσημης Εφημερίδας).

(32) Η υποστήριξη και η διατήρηση ενός αξιόπιστου, ανθεκτικού και ασφαλούς συστήματος ονομάτων χώρου (DNS) αποτελούν βασικό παράγοντα για τη διασφάλιση της ακεραιότητας του διαδικτύου και είναι ουσιαστικής σημασίας για τη συνεχή και σταθερή λειτουργία του, από την οποία εξαρτάται η ψηφιακή οικονομία και κοινωνία. Συνεπώς, η παρούσα οδηγία θα πρέπει να εφαρμόζεται στα μητρώα ονομάτων χώρου ανωτάτου επιπέδου (TLD) και στους παρόχους υπηρεσιών DNS που πρέπει να νοούνται ως οντότητες που παρέχουν δημόσια διαθέσιμες υπηρεσίες αναδρομικής επίλυσης ονομάτων χώρου για τελικούς χρήστες του διαδικτύου ή αυθεντικές υπηρεσίες επίλυσης ονομάτων χώρου για χρήση από τρίτους. Η παρούσα οδηγία δεν θα πρέπει να εφαρμόζεται σε εξυπηρετητές ονομάτων ρίζας (root name servers).

(33) Οι υπηρεσίες υπολογιστικού νέφους θα πρέπει να καλύπτουν ψηφιακές υπηρεσίες που καθιστούν δυνατή τη διαχείριση κατά παραγγελία και την ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενη και ελαστική δεξαμενή διαμοιραζόμενων υπολογιστικών πόρων, συμπεριλαμβανομένων και των πόρων που είναι κατανεμημένοι σε διάφορες τοποθεσίες. Οι υπολογιστικοί πόροι περιλαμβάνουν πόρους όπως δίκτυα, εξυπηρετητές ή άλλες υποδομές, λειτουργικά συστήματα, λογισμικό, αποθήκευση, εφαρμογές και υπηρεσίες. Τα μοντέλα υπηρεσιών υπολογιστικού νέφους περιλαμβάνουν, μεταξύ άλλων, την υποδομή ως υπηρεσία (IaaS), την πλατφόρμα ως υπηρεσία (PaaS), το λογισμικό ως υπηρεσία (SaaS) και το δίκτυο ως υπηρεσία (NaaS). Τα μοντέλα ανάπτυξης της νεφοϋπολογιστικής θα πρέπει να περιλαμβάνουν το ιδιωτικό, το κοινοτικό, το δημόσιο και το υβριδικό υπολογιστικό νέφος. Τα μοντέλα υπηρεσιών και ανάπτυξης υπολογιστικού νέφους έχουν την ίδια έννοια με τους όρους παροχής υπηρεσιών και μοντέλων ανάπτυξης που ορίζονται στο πρότυπο ISO/IEC 17788:2014. Η ικανότητα του χρήστη του υπολογιστικού νέφους να λαμβάνει μονομερώς με ίδια μέσα υπολογιστικές ικανότητες, όπως ο χρόνος εξυπηρετητή ή η δικτυακή αποθήκευση, χωρίς ανθρώπινη αλληλεπίδραση από τον πάροχο υπηρεσιών νεφοϋπολογιστικής, θα μπορούσε να περιγραφεί ως διαχείριση κατά παραγγελία.

Ο όρος «ευρεία εξ αποστάσεως πρόσβαση» χρησιμοποιείται για να περιγράψει ότι οι δυνατότητες υπολογιστικού νέφους παρέχονται μέσω του δικτύου και είναι προσβάσιμες μέσω μηχανισμών που προωθούν τη χρήση ετερογενών πλατφορμών τύπου thin ή thick client, συμπεριλαμβανομένων κινητών τηλεφώνων, ταμπλετών, φορητών υπολογιστών και σταθμών εργασίας. Ο όρος «κλιμακοθετήσιμο» αναφέρεται σε υπολογιστικούς πόρους που κατανέμονται με ευελιξία από τον πάροχο των υπηρεσιών νεφοϋπολογιστικής, ανεξαρτήτως της γεωγραφικής θέσης των πόρων, προκειμένου να αντιμετωπιστούν διακυμάνσεις στη ζήτηση. Ο όρος «ελαστικό σύνολο» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που παρέχονται και γίνονται διαθέσιμοι ανάλογα με τη ζήτηση προκειμένου να καταστεί δυνατή η ταχεία αύξηση και μείωση των διαθέσιμων πόρων ανάλογα με τον φόρτο εργασίας. Ο όρος «διαμοιραζόμενοι» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που παρέχονται σε πολλούς χρήστες που μοιράζονται μία κοινή πρόσβαση στην υπηρεσία, αλλά όπου η επεξεργασία εκτελείται χωριστά για κάθε χρήστη, παρόλο που η υπηρεσία παρέχεται από τον ίδιο ηλεκτρονικό εξοπλισμό. Ο όρος «κατανεμημένοι» χρησιμοποιείται για να περιγράψει υπολογιστικούς πόρους που βρίσκονται σε διαφορετικούς χωρικά δικτυωμένους υπολογιστές ή συσκευές και οι οποίοι επικοινωνούν και συντονίζονται μεταξύ τους μέσω διαβίβασης μηνυμάτων.

(34) Δεδομένης της ανάδυσης καινοτόμων τεχνολογιών και νέων επιχειρηματικών μοντέλων, αναμένεται να εμφανιστούν στην εσωτερική αγορά νέα μοντέλα υπηρεσιών και ανάπτυξης υπολογιστικού νέφους τα οποία θα ανταποκρίνονται στις εξελισσόμενες ανάγκες των πελατών. Στο πλαίσιο αυτό, οι υπηρεσίες νεφοϋπολογιστικής μπορούν να παρέχονται σε έντονα κατανεμημένη μορφή, ακόμη εγγύτερα στον τόπο παραγωγής ή συλλογής των δεδομένων, μεταβαίνοντας έτσι από το παραδοσιακό μοντέλο σε ένα έντονα κατανεμημένο μοντέλο (υπολογιστική παρυφών).

(35) Οι υπηρεσίες που παρέχονται από τους παρόχους υπηρεσιών κέντρων δεδομένων ενδέχεται να μην παρέχονται πάντοτε στη μορφή υπηρεσιών υπολογιστικού νέφους. Ως εκ τούτου, τα κέντρα δεδομένων ενδέχεται να μην αποτελούν πάντοτε μέρος της υποδομής νεφοϋπολογιστικής. Για τη διαχείριση όλων των κινδύνων που αφορούν στην ασφάλεια των συστημάτων δικτύου και πληροφοριών, η παρούσα οδηγία θα πρέπει επομένως να καλύπτει και τους παρόχους τέτοιων υπηρεσιών κέντρων δεδομένων που δεν είναι υπηρεσίες υπολογιστικού νέφους. Για τους σκοπούς της παρούσας οδηγίας, ο όρος «υπηρεσία κέντρων δεδομένων» θα πρέπει να καλύπτει την παροχή υπηρεσίας που περιλαμβάνει δομές, ή ομάδες δομών, που προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία της τεχνολογίας πληροφοριών («ΤΠ») και του εξοπλισμού δικτύου που παρέχει υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ηλεκτρικής ενέργειας και περιβαλλοντικού ελέγχου. Ο όρος «υπηρεσία κέντρων δεδομένων» δεν θα πρέπει να ισχύει για ενδοεπιχειρησιακά εταιρικά κέντρα δεδομένων που ανήκουν στην οικεία οντότητα και λειτουργούν για ίδιους σκοπούς.

(36) Οι ερευνητικές δραστηριότητες διαδραματίζουν καίριο ρόλο στην ανάπτυξη νέων προϊόντων και διαδικασιών. Πολλές από τις δραστηριότητες αυτές διεξάγονται από οντότητες που μοιράζονται, διαθέτουν ή εκμεταλλεύονται τα αποτελέσματα της έρευνάς τους για εμπορικούς σκοπούς. Συνεπώς, οι εν λόγω οντότητες μπορούν να αποτελέσουν σημαντικούς παράγοντες στις αλυσίδες αξίας, γεγονός που καθιστά την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους αναπόσπαστο μέρος της συνολικής κυβερνοασφάλειας της εσωτερικής αγοράς. Οι ερευνητικοί οργανισμοί θα πρέπει να νοούνται ως φορείς που εστιάζουν το κύριο μέρος των δραστηριοτήτων τους στη διεξαγωγή εφαρμοσμένης έρευνας ή πειραματικής

ανάπτυξης, κατά την έννοια του εγχειριδίου Frascati 2015 του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης: Κατευθυντήριες γραμμές για τη συλλογή και την υποβολή δεδομένων σχετικά με την έρευνα και την πειραματική ανάπτυξη, με σκοπό την εκμετάλλευση των αποτελεσμάτων τους για εμπορικούς σκοπούς, όπως η κατασκευή ή η ανάπτυξη ενός προϊόντος, ή μιας διαδικασίας, η παροχή μιας υπηρεσίας, ή η εμπορία αυτών.

(37) Οι αυξανόμενες αλληλεξαρτήσεις είναι αποτέλεσμα ενός ολοένα και περισσότερο διασυνοριακού και αλληλεξαρτώμενου δικτύου παροχής υπηρεσιών που χρησιμοποιεί βασικές υποδομές σε ολόκληρη την Ένωση σε τομείς όπως της ενέργειας, των μεταφορών, των ψηφιακών υποδομών, του πόσιμου νερού και των λυμάτων, της υγείας, ορισμένων πτυχών της δημόσιας διοίκησης, καθώς και του διαστήματος, στον βαθμό που αφορά την παροχή ορισμένων υπηρεσιών που εξαρτώνται από επίγειες υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει είτε σε κράτη μέλη είτε σε ιδιώτες, και, ως εκ τούτου, δεν καλύπτει τις υποδομές των οποίων η κυριότητα, η διαχείριση και η λειτουργία ανήκει στην Ένωση, ή γίνεται εξ ονόματος αυτής, στο πλαίσιο των διαστημικών προγραμμάτων της. Λόγω των αλληλεξαρτήσεων αυτών, οποιαδήποτε διατάραξη, ακόμη και αν αρχικά περιοριζόταν σε μία οντότητα ή σε έναν τομέα, μπορεί να έχει ευρύτερες αλυσιδωτές επιπτώσεις, με δυνητικά μεγάλης κλίμακας και μακροχρόνιο αρνητικό αντίκτυπο στην παροχή υπηρεσιών σε ολόκληρη την εσωτερική αγορά. Οι ενταθείσες κυβερνοεπιθέσεις στη διάρκεια της πανδημίας της COVID-19 κατέδειξαν την τρωτότητα των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών απέναντι σε κινδύνους χαμηλής πιθανότητας.

(38) Δεδομένων των διαφορών στις εθνικές δομές διακυβέρνησης και προκειμένου να διασφαλιστούν οι ήδη υφιστάμενες τομεακές ρυθμίσεις ή οι εποπτικοί και ρυθμιστικοί φορείς της Ένωσης, τα κράτη μέλη θα πρέπει να είναι σε θέση να ορίσουν ή να συστήσουν μία ή περισσότερες αρμόδιες αρχές υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα δυνάμει της παρούσας οδηγίας.

(39) Για τη διευκόλυνση της διασυνοριακής συνεργασίας και επικοινωνίας μεταξύ των αρχών, και για να καταστεί δυνατή η αποτελεσματική εφαρμογή της παρούσας οδηγίας, είναι ανάγκη κάθε κράτος μέλος να ορίζει ένα ενιαίο σημείο επαφής υπεύθυνο για τον συντονισμό θεμάτων σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών και με τη διασυνοριακή συνεργασία σε επίπεδο Ένωσης.

(40) Τα ενιαία σημεία επαφής θα πρέπει να διασφαλίζουν την αποτελεσματική διασυνοριακή συνεργασία με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Επιτροπή και τον ENISA. Συνεπώς, τα ενιαία σημεία επαφής θα πρέπει να είναι επιφορτισμένα με τη διαβίβαση των κοινοποιήσεων σημαντικών περιστατικών με διασυνοριακό αντίκτυπο στα ενιαία σημεία επαφής άλλων επηρεαζόμενων κρατών μελών κατόπιν αιτήματος της CSIRT ή της αρμόδιας αρχής. Σε εθνικό επίπεδο, τα ενιαία σημεία επαφής θα πρέπει να επιτρέπουν την ομαλή διατομεακή συνεργασία με άλλες αρμόδιες αρχές. Τα ενιαία σημεία επαφής θα μπορούσαν επίσης να είναι οι αποδέκτες σχετικών πληροφοριών σχετικά με περιστατικά που αφορούν χρηματοπιστωτικές οντότητες από τις αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554, τις οποίες θα πρέπει να είναι σε θέση να διαβιβάζουν, κατά περίπτωση, στις CSIRT ή στις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας.

(41) Τα κράτη μέλη θα πρέπει να είναι επαρκώς εξοπλισμένα, όσον αφορά τόσο τις τεχνικές όσο και τις οργανωτικές ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση περιστατικών και κινδύνων, καθώς και για τον μετριασμό των επιπτώσεών τους. Τα κράτη μέλη θα πρέπει επομένως να συστήσουν ή ορίσουν μία ή περισσότερες CSIRT δυνάμει της παρούσας οδηγίας και να διασφαλίσουν ότι διαθέτουν επαρκείς πόρους και τεχνικές ικανότητες. Οι CSIRT θα πρέπει να συμμορφώνονται με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία, προκειμένου να διασφαλίζονται αποτελεσματικές και συμβατές ικανότητες αντιμετώπισης περιστατικών και κινδύνων και να διασφαλίζεται αποτελεσματική συνεργασία σε επίπεδο Ένωσης. Τα κράτη μέλη δύνανται να ορίσουν υπάρχουσες ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (Computer Emergency Response Teams — CERT) ως CSIRT. Προκειμένου να ενισχυθεί η σχέση εμπιστοσύνης μεταξύ των οντοτήτων και των CSIRT, στις περιπτώσεις που μια CSIRT αποτελεί μέρος της αρμόδιας αρχής, τα κράτη μέλη θα πρέπει να μπορούν να εξετάσουν το ενδεχόμενο λειτουργικού διαχωρισμού μεταξύ των επιχειρησιακών καθηκόντων που επιτελούν οι CSIRT, ιδίως όσον αφορά την ανταλλαγή πληροφοριών και τη στήριξη προς τις οντότητες, και των εποπτικών δραστηριοτήτων των αρμόδιων αρχών.

(42) Οι CSIRT είναι επιφορτισμένες με τον χειρισμό περιστατικών. Αυτό περιλαμβάνει την επεξεργασία μεγάλων όγκων ενίοτε ευαίσθητων δεδομένων. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι CSIRT διαθέτουν υποδομή για την ανταλλαγή και επεξεργασία πληροφοριών, καθώς και καλά εξοπλισμένο προσωπικό, ώστε να διασφαλίζονται η εμπιστευτικότητα και η αξιοπιστία των δραστηριοτήτων τους. Οι CSIRT θα μπορούσαν επίσης να θεσπίσουν σχετικούς κώδικες δεοντολογίας.

(43) Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, οι CSIRT θα πρέπει να είναι σε θέση να παρέχουν, σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, εξ ονόματος και κατόπιν αιτήματος βασικής ή σημαντικής οντότητας, προληπτική σάρωση των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή των υπηρεσιών τους. Κατά περίπτωση, τα κράτη μέλη θα πρέπει να στοχεύουν στην εξασφάλιση του ίδιου επιπέδου τεχνικών ικανοτήτων για όλες τις τομεακές CSIRT. Τα κράτη μέλη θα πρέπει να μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των CSIRT τους.

(44) Οι CSIRT θα πρέπει να έχουν τη δυνατότητα, κατόπιν αιτήματος μιας βασικής ή σημαντικής οντότητας, να παρακολουθούν τα στοιχεία της οντότητας που βρίσκονται στο διαδίκτυο, τόσο εντός όσο και εκτός των εγκαταστάσεων, προκειμένου να εντοπίζουν, να κατανοούν και να διαχειρίζονται τους συνολικούς οργανωτικούς κινδύνους της οντότητας όσον αφορά τις νεοεντοπισθείσες προσβολές της αλυσίδας εφοδιασμού ή τις κρίσιμες τρωτότητες. Η οντότητα θα πρέπει να ενθαρρύνεται να γνωστοποιεί στην CSIRT κατά πόσον διαχειρίζεται προνομιακή διεπαφή διαχείρισης, καθώς αυτό θα μπορούσε να επηρεάσει την ταχύτητα λήψης μέτρων μετριασμού.

(45) Δεδομένης της σημασίας της διεθνούς συνεργασίας για την κυβερνοασφάλεια, οι CSIRT θα πρέπει να έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας πέραν του δικτύου CSIRT που θεσπίζεται με την παρούσα οδηγία. Κατά συνέπεια, για τους σκοπούς της εκτέλεσης των καθηκόντων τους, οι CSIRT και οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να ανταλλάσσουν πληροφορίες, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, με τις εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές ή με αρμόδιες αρχές τρίτων χωρών, υπό την προϋπόθεση ότι πληρούνται οι προϋποθέσεις της ενωσιακής νομοθεσίας για την προστασία των δεδομένων για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, μεταξύ άλλων εκείνες του άρθρου 49 του κανονισμού (ΕΕ) 2016/679.

(46) Είναι ουσιαστικής σημασίας η εξασφάλιση επαρκών πόρων για την επίτευξη των στόχων της παρούσας οδηγίας και για να παρασχεθεί στις αρμόδιες αρχές και στις CSIRT η δυνατότητα να εκτελούν τα καθήκοντα που ορίζονται στο παρόν. Τα κράτη μέλη μπορούν να θεσπίσουν σε εθνικό επίπεδο χρηματοδοτικό μηχανισμό για την κάλυψη των αναγκαίων δαπανών σε σχέση με την εκτέλεση των καθηκόντων των δημόσιων φορέων που είναι αρμόδιοι για την κυβερνοασφάλεια στο κράτος μέλος σύμφωνα με την παρούσα οδηγία. Ο εν λόγω μηχανισμός θα πρέπει να συμμορφώνεται με το δίκαιο της Ένωσης, να είναι αναλογικός και να μην εισάγει διακρίσεις, και να λαμβάνει υπόψη τις διαφορετικές προσεγγίσεις για την παροχή ασφαλών υπηρεσιών.

(47) Το δίκτυο CSIRT θα πρέπει να συνεχίσει να συμβάλλει στην ενίσχυση της αξιοπιστίας και της εμπιστοσύνης και να προωθεί την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία μεταξύ των κρατών μελών. Για να ενισχυθεί η επιχειρησιακή συνεργασία σε επίπεδο Ένωσης, το δίκτυο CSIRT θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλέσει όργανα και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως η Ευρωπόλ, να συμμετάσχουν στις εργασίες του.

(48) Για την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας, οι εθνικές στρατηγικές κυβερνοασφάλειας που απαιτούνται βάσει της παρούσας οδηγίας θα πρέπει να αποτελούνται από συνεκτικά πλαίσια που παρέχουν στρατηγικούς στόχους και προτεραιότητες στον τομέα της κυβερνοασφάλειας και της διακυβέρνησης για την επίτευξή τους. Οι στρατηγικές αυτές μπορούν να αποτελούνται από ένα ή περισσότερα νομοθετικά ή μη νομοθετικά μέσα.

(49) Οι πολιτικές κυβερνοϋγιεινής παρέχουν τα θεμέλια για την προστασία των υποδομών δικτυακών και πληροφοριακών συστημάτων, του υλικού, του λογισμικού και της ασφάλειας των διαδικτυακών εφαρμογών, καθώς και των δεδομένων των επιχειρήσεων ή των τελικών χρηστών στα οποία βασίζονται οι οντότητες. Οι πολιτικές κυβερνοϋγιεινής που περιλαμβάνουν κοινό βασικό σύνολο πρακτικών, συμπεριλαμβανομένων ενημερώσεων λογισμικού και αναβαθμίσεων υλικού, αλλαγών κωδικού πρόσβασης, διαχείρισης νέων εγκαταστάσεων, περιορισμού των λογαριασμών πρόσβασης σε επίπεδο διαχειριστή και δημιουργίας αντιγράφων ασφάλειας δεδομένων, δημιουργούν ένα προληπτικό πλαίσιο ετοιμότητας και γενικής ασφάλειας και προστασίας σε περίπτωση περιστατικών ή κυβερνοαπειλών. Ο ENISA θα πρέπει να παρακολουθεί και να αναλύει τις πολιτικές κυβερνοϋγιεινής των κρατών μελών.

(50) Η ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας και η κυβερνοϋγιεινή είναι ουσιαστικής σημασίας για την ενίσχυση του επιπέδου κυβερνοασφάλειας εντός της Ένωσης, ιδίως μέσα από το πρίσμα του αυξανόμενου αριθμού συνδεδεμένων συσκευών που χρησιμοποιούνται όλο και περισσότερο σε κυβερνοεπιθέσεις. Θα πρέπει να καταβληθούν προσπάθειες για την ενίσχυση της συνολικής ευαισθητοποίησης σχετικά με τους κινδύνους που συνδέονται με τα εν λόγω ιατροτεχνολογικά προϊόντα, ενώ οι αξιολογήσεις σε επίπεδο Ένωσης θα μπορούσαν να συμβάλουν στη διασφάλιση κοινής αντίληψης των κινδύνων αυτών στην εσωτερική αγορά.

(51) Τα κράτη μέλη θα πρέπει να ενθαρρύνουν τη χρήση κάθε καινοτόμου τεχνολογίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, η χρήση της οποίας θα μπορούσε να βελτιώσει τον εντοπισμό και την πρόληψη κυβερνοεπιθέσεων, καθιστώντας δυνατή την αποτελεσματικότερη διοχέτευση πόρων για την αντιμετώπιση κυβερνοεπιθέσεων. Για το σκοπό αυτό, τα κράτη μέλη θα πρέπει να ενθαρρύνουν, στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια, τις δραστηριότητες έρευνας και ανάπτυξης για τη διευκόλυνση της χρήσης των εν λόγω τεχνολογιών, ιδίως εκείνων που σχετίζονται με αυτοματοποιημένα ή ημιαυτοματοποιημένα εργαλεία κυβερνοασφάλειας, και, κατά περίπτωση, την ανταλλαγή δεδομένων που απαιτούνται για την κατάρτιση των χρηστών της εν λόγω τεχνολογίας και για τη βελτίωσή της. Η χρήση κάθε καινοτόμου τεχνολογίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, θα πρέπει να συμμορφώνεται με την ενωσιακή νομοθεσία για την προστασία των δεδομένων, συμπεριλαμβανομένων των αρχών προστασίας των δεδομένων που αφορούν την ακρίβεια των δεδομένων, την ελαχιστοποίηση των δεδομένων, τη δικαιοσύνη και τη διαφάνεια, καθώς και την ασφάλεια των δεδομένων, όπως η τελευταίας τεχνολογίας κρυπτογράφηση. Οι απαιτήσεις προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού που ορίζονται στον κανονισμό (ΕΕ) 2016/679 θα πρέπει να αξιοποιηθούν πλήρως.

(52) Τα εργαλεία και οι εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα μπορούν να συμβάλουν σε υψηλότερο βαθμό διαφάνειας και δύνανται να έχουν θετικό αντίκτυπο στην αποδοτικότητα της βιομηχανικής καινοτομίας. Τα ανοικτά πρότυπα διευκολύνουν τη διαλειτουργικότητα μεταξύ των εργαλείων ασφάλειας, ωφελώντας την ασφάλεια των ενδιαφερόμενων μερών του βιομηχανικού κλάδου. Τα εργαλεία και οι εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα μπορούν να αξιοποιήσουν την ευρύτερη κοινότητα των φορέων ανάπτυξης, καθιστώντας δυνατή τη διαφοροποίηση των προμηθευτών. Ο ανοικτός κώδικας μπορεί να οδηγήσει σε διαφανέστερη διαδικασία επαλήθευσης των εργαλείων που σχετίζονται με την κυβερνοασφάλεια και σε μια διαδικασία εντοπισμού ευπαθειών σε επίπεδο κοινότητας. Συνεπώς, τα κράτη μέλη θα πρέπει να μπορούν να προωθήσουν τη χρήση λογισμικού ανοικτού κώδικα και ανοικτών προτύπων με την εφαρμογή πολιτικών που συνδέονται με τη χρήση ανοικτών δεδομένων και ανοικτού κώδικα στο πλαίσιο της ασφάλειας μέσω διαφάνειας. Οι πολιτικές που προωθούν την εισαγωγή και τη βιώσιμη χρήση εργαλείων κυβερνοασφάλειας ανοικτού κώδικα έχουν ιδιαίτερη σημασία για τις μικρές και μεσαίες επιχειρήσεις που αντιμετωπίζουν σημαντικό κόστος υλοποίησης, το οποίο θα μπορούσε να ελαχιστοποιηθεί με τη μείωση της ανάγκης για συγκεκριμένες εφαρμογές ή εργαλεία.

(53) Οι υπηρεσίες κοινής ωφελείας συνδέονται όλο και περισσότερο με ψηφιακά δίκτυα στις πόλεις, με σκοπό τη βελτίωση των δικτύων αστικών μεταφορών, την αναβάθμιση των εγκαταστάσεων ύδρευσης και διάθεσης αποβλήτων και την αύξηση της αποδοτικότητας του φωτισμού και της θέρμανσης των κτιρίων. Αυτές οι ψηφιοποιημένες υπηρεσίες κοινής ωφελείας είναι ευπαθείς σε κυβερνοεπιθέσεις και διατρέχουν τον κίνδυνο, σε περίπτωση επιτυχούς κυβερνοεπίθεσης, να βλάψουν τους πολίτες σε μεγάλη κλίμακα λόγω της διασύνδεσής τους. Τα κράτη μέλη θα πρέπει να αναπτύξουν μια πολιτική που θα αντιμετωπίζει την ανάπτυξη των εν λόγω συνδεδεμένων ή έξυπνων πόλεων και τις πιθανές επιπτώσεις τους στην κοινωνία, στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια.

(54) Τα τελευταία χρόνια, η Ένωση αντιμετώπισε εκθετική αύξηση των επιθέσεων λυτρισμικού, στις οποίες το κακόβουλο λογισμικό κρυπτογραφεί δεδομένα και συστήματα και απαιτεί την καταβολή λύτρων για την αποδέσμευση. Η αυξανόμενη συχνότητα και σοβαρότητα των επιθέσεων λυτρισμικού μπορεί να οφείλεται σε διάφορους παράγοντες, όπως οι διαφορετικές μορφές επιθέσεων, τα εγκληματικά επιχειρηματικά μοντέλα για την πραγματοποίηση επιθέσεων λυτρισμικού ως παροχή υπηρεσίας και τα κρυπτονομίσματα, οι απαιτήσεις λύτρων και η αύξηση των επιθέσεων στην αλυσίδα εφοδιασμού. Τα κράτη μέλη θα πρέπει να αναπτύξουν πολιτική για την αντιμετώπιση της αύξησης των επιθέσεων λυτρισμικού στο πλαίσιο της εθνικής στρατηγικής τους για την κυβερνοασφάλεια.

(55) Οι συμπράξεις δημόσιου και ιδιωτικού τομέα («ΣΔΙΤ») στον τομέα της κυβερνοασφάλειας μπορούν να προσφέρουν κατάλληλο πλαίσιο για την ανταλλαγή γνώσεων, την ανταλλαγή βέλτιστων πρακτικών και την καθιέρωση κοινού επιπέδου κατανόησης μεταξύ των ενδιαφερόμενων μερών. Τα κράτη μέλη θα πρέπει να θεσπίσουν πολιτικές που θα στηρίζουν τη δημιουργία ΣΔΙΤ για την κυβερνοασφάλεια. Οι πολιτικές αυτές θα πρέπει να αποσαφηνίζουν, μεταξύ άλλων, το πεδίο εφαρμογής και τα ενδιαφερόμενα μέρη, το μοντέλο διακυβέρνησης, τις διαθέσιμες επιλογές χρηματοδότησης και την αλληλεπίδραση μεταξύ των συμμετεχόντων ενδιαφερόμενων μερών σε σχέση με τις ΣΔΙΤ. Οι ΣΔΙΤ μπορούν να αξιοποιήσουν την εμπειρογνωσία οντοτήτων του ιδιωτικού τομέα για να συνδράμουν τις αρμόδιες αρχές στην ανάπτυξη προηγμένων υπηρεσιών και διαδικασιών που περιλαμβάνουν, μεταξύ άλλων, την ανταλλαγή πληροφοριών, έγκαιρες προειδοποιήσεις, ασκήσεις αντιμετώπισης κυβερνοαπειλών και περιστατικών στον κυβερνοχώρο, τη διαχείριση κρίσεων και τον σχεδιασμό ανθεκτικότητας.

(56) Τα κράτη μέλη θα πρέπει, στις εθνικές στρατηγικές τους για την κυβερνοασφάλεια, να αντιμετωπίζουν τις ειδικές ανάγκες των μικρών και μεσαίων επιχειρήσεων στον τομέα της κυβερνοασφάλειας. Οι μικρές και μεσαίες επιχειρήσεις αντιπροσωπεύουν, σε επίπεδο Ένωσης, μεγάλο ποσοστό της βιομηχανικής και επιχειρηματικής αγοράς και συχνά δυσκολεύονται να προσαρμοστούν στις νέες επιχειρηματικές πρακτικές σε έναν πιο συνδεδεμένο κόσμο, και στο ψηφιακό περιβάλλον, με τους εργαζομένους να εργάζονται κατ' οίκον και τις επιχειρήσεις να δραστηριοποιούνται διαρκώς περισσότερο στο διαδίκτυο. Ορισμένες μικρές και μεσαίες επιχειρήσεις αντιμετωπίζουν συγκεκριμένες προκλήσεις κυβερνοασφάλειας, όπως χαμηλή κυβερνοευαισθητοποίηση, έλλειψη τηλεματικής ασφάλειας ΤΠ, υψηλό κόστος λύσεων κυβερνοασφάλειας και αυξημένο επίπεδο απειλών, όπως το λυτρισμικό, για τις οποίες θα πρέπει να λαμβάνουν καθοδήγηση και βοήθεια. Οι μικρές και μεσαίες επιχειρήσεις καθίστανται όλο και περισσότερο στόχος επιθέσεων στην αλυσίδα εφοδιασμού λόγω των λιγότερο αυστηρών μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και της διαχείρισης επιθέσεων, καθώς και λόγω του γεγονότος ότι διαθέτουν περιορισμένους πόρους ασφάλειας. Οι εν λόγω επιθέσεις στην αλυσίδα εφοδιασμού όχι μόνο έχουν αντίκτυπο στις μικρές και μεσαίες επιχειρήσεις και στις δραστηριότητές

τους μεμονωμένα, αλλά μπορούν επίσης να έχουν αλυσιδωτές επιπτώσεις σε μεγαλύτερες επιθέσεις κατά οντοτήτων στις οποίες παρείχαν προμήθειες. Τα κράτη μέλη θα πρέπει, μέσω των εθνικών στρατηγικών τους για την κυβερνοασφάλεια, να βοηθούν τις μικρές και μεσαίες επιχειρήσεις να αντιμετωπίσουν τις προκλήσεις που αντιμετωπίζουν οι αλυσίδες εφοδιασμού τους. Τα κράτη μέλη θα πρέπει να διαθέτουν ένα σημείο επαφής για τις μικρές και μεσαίες επιχειρήσεις σε εθνικό ή περιφερειακό επίπεδο, το οποίο είτε θα παρέχει καθοδήγηση και συνδρομή στις μικρές και μεσαίες επιχειρήσεις είτε θα τις κατευθύνει στους κατάλληλους φορείς για καθοδήγηση και συνδρομή όσον αφορά ζητήματα κυβερνοασφάλειας. Τα κράτη μέλη ενθαρρύνονται επίσης να προσφέρουν υπηρεσίες όπως η παροχή δυνατότητας για διαμόρφωση ιστοτόπων και καταγραφή δεδομένων σε πολύ μικρές και μικρές επιχειρήσεις που δεν διαθέτουν τις σχετικές ικανότητες.

(57) Στο πλαίσιο των εθνικών στρατηγικών τους για την ασφάλεια στον κυβερνοχώρο, τα κράτη μέλη θα πρέπει να εγκρίνουν πολιτικές για την προώθηση της ενεργητικής κυβερνοπροστασίας στο πλαίσιο μιας ευρύτερης αμυντικής στρατηγικής. Σε αντιδιαστολή με την εκ των υστέρων ανταπόκριση, η ενεργητική κυβερνοπροστασία συνίσταται στην πρόληψη, τον εντοπισμό, την παρακολούθηση, την ανάλυση και τον μετριασμό των παραβιάσεων της ασφάλειας των δικτύων με ενεργό τρόπο, σε συνδυασμό με τη χρήση ικανοτήτων που αναπτύσσονται εντός και εκτός του δικτύου των θυμάτων. Αυτό θα μπορούσε να περιλαμβάνει την παροχή δωρεάν υπηρεσιών ή εργαλείων σε ορισμένες οντότητες από τα κράτη μέλη, συμπεριλαμβανομένων των ελέγχων αυτοεξυπηρέτησης, των εργαλείων ανίχνευσης και των υπηρεσιών απόσυρσης. Η ικανότητα ταχείας και αυτόματης ανταλλαγής και κατανόησης πληροφοριών και αναλύσεων απειλών, προειδοποιήσεων για δραστηριότητες στον κυβερνοχώρο, και δράσης αντιμετώπισης είναι ζωτικής σημασίας για να καταστεί δυνατή η ενότητα των προσπαθειών για την επιτυχή πρόληψη, ανίχνευση, αντιμετώπιση και παρεμπόδιση επιθέσεων κατά συστημάτων δικτύου και πληροφοριών. Η ενεργητική κυβερνοπροστασία βασίζεται σε μια αμυντική στρατηγική που αποκλείει τα επιθετικά μέτρα.

(58) Δεδομένου ότι η εκμετάλλευση των τρωτοτήτων στα συστήματα δικτύου και πληροφοριών μπορεί να προκαλέσει σημαντικές διαταράξεις και βλάβες, ο άμεσος εντοπισμός και η διόρθωση αυτών των τρωτοτήτων αποτελεί σημαντικό παράγοντα μείωσης του κινδύνου. Οι οντότητες που αναπτύσσουν ή διαχειρίζονται συστήματα δικτύου και πληροφοριών θα πρέπει, συνεπώς, να θεσπίσουν κατάλληλες διαδικασίες για την αντιμετώπιση των τρωτοτήτων όταν εντοπίζονται. Δεδομένου ότι οι ευπάθειες συχνά εντοπίζονται και γνωστοποιούνται από τρίτους, ο κατασκευαστής ή ο πάροχος προϊόντων ή υπηρεσιών ΤΠΕ θα πρέπει επίσης να θεσπίσει τις αναγκαίες διαδικασίες για τη λήψη πληροφοριών από τρίτους σχετικά με ευπάθειες. Στο πλαίσιο αυτό, τα διεθνή πρότυπα ISO/IEC 30111 και ISO/IEC 29147 παρέχουν καθοδήγηση σχετικά με τον χειρισμό τρωτοτήτων και τη γνωστοποίηση τρωτοτήτων. Η ενίσχυση του συντονισμού μεταξύ των αναφερόντων φυσικών και νομικών προσώπων και των κατασκευαστών ή παρόχων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ είναι ιδιαίτερα σημαντική για τον σκοπό της διευκόλυνσης του εθελοντικού πλαισίου γνωστοποίησης τρωτοτήτων. Η συντονισμένη γνωστοποίηση τρωτοτήτων καθορίζει μια δομημένη διαδικασία μέσω της οποίας αναφέρονται στον κατασκευαστή ή τον πάροχο των δυνητικά ευάλωτων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ οι τρωτότητες, κατά τρόπο που να του επιτρέπει να διαγιγνώσκει και να αποκαθιστά την τρωτότητα πριν από τη γνωστοποίηση λεπτομερών πληροφοριών για τρωτότητες σε τρίτους ή στο κοινό. Η συντονισμένη γνωστοποίηση τρωτοτήτων θα πρέπει επίσης να περιλαμβάνει συντονισμό μεταξύ του αναφέροντος φυσικού ή νομικού προσώπου και του κατασκευαστή ή του παρόχου των δυνητικά ευάλωτων προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ όσον αφορά το χρονοδιάγραμμα αποκατάστασης και δημοσίευσης των τρωτοτήτων.

(59) Η Επιτροπή, ο ENISA και τα κράτη μέλη θα πρέπει να συνεχίσουν να προωθούν την ευθυγράμμιση με διεθνή πρότυπα και υπάρχουσες βέλτιστες πρακτικές της βιομηχανίας στον τομέα της διαχείρισης κινδύνων κυβερνοασφάλειας, για παράδειγμα στους τομείς των αξιολογήσεων ασφάλειας της αλυσίδας εφοδιασμού, της ανταλλαγής πληροφοριών και της γνωστοποίησης τρωτοτήτων.

(60) Τα κράτη μέλη, σε συνεργασία με τον ENISA, οφείλουν να λάβουν μέτρα για να διευκολύνουν τη συντονισμένη γνωστοποίηση τρωτοτήτων με τη θέσπιση σχετικής εθνικής πολιτικής. Στο πλαίσιο της εθνικής πολιτικής τους, τα κράτη μέλη θα πρέπει να στοχεύουν στην αντιμετώπιση, στο μέτρο του δυνατού, των προκλήσεων που αντιμετωπίζουν πρόσωπα που ερευνούν ευπάθειες, συμπεριλαμβανομένης της ενδεχόμενης έκθεσής τους σε ποινική ευθύνη, σύμφωνα με την εθνική νομοθεσία τους. Δεδομένου ότι τα φυσικά και νομικά πρόσωπα που ερευνούν ευπάθειες θα μπορούσαν σε ορισμένα κράτη μέλη να εκτεθούν σε ποινική και αστική ευθύνη, τα κράτη μέλη ενθαρρύνονται να εγκρίνουν κατευθυντήριες γραμμές όσον αφορά τη μη δίωξη των ερευνητών στον τομέα της ασφάλειας των πληροφοριών και την απαλλαγή από την αστική ευθύνη για τις δραστηριότητές τους.

(61) Τα κράτη μέλη θα πρέπει να ορίσουν μια από τις CSIRT τους ως συντονιστή η οποία να ενεργεί ως αξιόπιστος ενδιάμεσος φορέας μεταξύ των αναφερόντων φυσικών ή νομικών προσώπων και των κατασκευαστών προϊόντων ΤΠΕ ή παρόχων υπηρεσιών ΤΠΕ, που ενδέχεται να επηρεαστούν από την τρωτότητα, όπου απαιτείται. Τα καθήκοντα της CSIRT που ορίσθηκε ως συντονιστής θα πρέπει να περιλαμβάνουν τον προσδιορισμό των οικείων οντοτήτων και την επικοινωνία με αυτές, την παροχή συνδρομής στα φυσικά ή νομικά πρόσωπα που αναφέρουν ευπάθειες, τη διαπραγμάτευση χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση τρωτοτήτων που επηρεάζουν πλείονες οντότητες (πολυμερής

συντονισμένη γνωστοποίηση ευπαθειών). Όταν η αναφερόμενη τρωτότητα θα μπορούσε να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, οι CSIRT που ορίσθηκαν ως συντονιστές θα πρέπει να συνεργάζονται στο πλαίσιο του δικτύου CSIRT, κατά περίπτωση.

(62) Η πρόσβαση σε ορθές και έγκαιρες πληροφορίες σχετικά με ευπάθειες που επηρεάζουν τα προϊόντα και τις υπηρεσίες ΤΠΕ συμβάλλει στην ενίσχυση της διαχείρισης κινδύνων κυβερνοασφάλειας. Οι πηγές δημόσια διαθέσιμων πληροφοριών σχετικά με τρωτότητες αποτελούν σημαντικό εργαλείο για τις οντότητες και τους χρήστες των υπηρεσιών τους, αλλά και για τις εθνικές αρμόδιες αρχές και τις CSIRT. Για τον λόγο αυτό, ο ENISA θα πρέπει να καταρτίσει μια ευρωπαϊκή βάση δεδομένων ευπαθειών όπου οι οντότητες, ανεξαρτήτως από το αν εμπίπτουν στο πεδίο της παρούσας οδηγίας, και οι προμηθευτές τους για συστήματα δικτύου και πληροφοριών, όπως επίσης οι αρμόδιες αρχές και οι CSIRT, μπορούν να δημοσιοποιούν και να καταχωρούν, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες ώστε να μπορούν οι χρήστες να λαμβάνουν κατάλληλα μέτρα μετριασμού. Σκοπός της εν λόγω βάσης δεδομένων είναι η αντιμετώπιση των μοναδικών προκλήσεων που συνιστούν οι κίνδυνοι κυβερνοασφάλειας για τις οντότητες στην Ένωση. Επιπλέον, ο ENISA θα πρέπει να θεσπίσει κατάλληλη διαδικασία σχετικά με τη διαδικασία δημοσίευσης, προκειμένου να δοθεί στις οντότητες ο χρόνος να λάβουν μέτρα μετριασμού όσον αφορά τις τρωτότητές τους και να εφαρμόσουν σύγχρονα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, καθώς και μηχαναγνώσιμα σύνολα δεδομένων και αντίστοιχες διεπαφές. Για να ενθαρρυνθεί η νοοτροπία γνωστοποίησης ευπαθειών, η γνωστοποίηση δεν θα πρέπει να βλάπτει το αναφέρον φυσικό ή νομικό πρόσωπο.

(63) Μολονότι υπάρχουν παρόμοια μητρώα ή βάσεις δεδομένων ευπαθειών, αυτά φιλοξενούνται και τηρούνται από οντότητες που δεν είναι εγκατεστημένες στην Ένωση. Μια ευρωπαϊκή βάση δεδομένων ευπαθειών που θα τηρείται από τον ENISA θα προσέφερε βελτιωμένη διαφάνεια όσον αφορά στη διαδικασία δημοσίευσης προτού κάποια ευπάθεια γίνει δημόσια γνωστή, καθώς και ανθεκτικότητα σε περίπτωση διατάραξης ή διακοπής της παροχής παρόμοιων υπηρεσιών. Προκειμένου, στο μέτρο του δυνατού, να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να επιδιωχθεί η συμπληρωματικότητα, ο ENISA θα πρέπει να διερευνήσει τη δυνατότητα σύναψης συμφωνιών διαρθρωμένης συνεργασίας με παρόμοια μητρώα ή βάσεις δεδομένων που υπάγονται στη δικαιοδοσία τρίτων χωρών. Ειδικότερα, ο ENISA θα πρέπει να διερευνήσει τη δυνατότητα στενής συνεργασίας με τους φορείς εκμετάλλευσης του συστήματος Κοινών Ευπαθειών και Εκτεθειμένων Σημείων (CVE).

(64) Η Ομάδα Συνεργασίας θα πρέπει να στηρίζει και να διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών, καθώς και να ενισχύει την εμπιστοσύνη μεταξύ των κρατών μελών. Η Ομάδα Συνεργασίας θα πρέπει να καταρτίζει ανά διετία πρόγραμμα εργασίας. Το πρόγραμμα εργασίας θα πρέπει να περιλαμβάνει τις ενέργειες που θα αναλάβει η Ομάδα Συνεργασίας για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα για την κατάρτιση του πρώτου προγράμματος εργασιών βάσει της παρούσας οδηγίας θα πρέπει να ευθυγραμμιστεί με το χρονοδιάγραμμα του τελευταίου προγράμματος εργασίας που θεσπίστηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148, προκειμένου να αποφευχθούν πιθανές διαταραχές στις εργασίες της ομάδας συνεργασίας.

(65) Κατά την κατάρτιση έγγραφων οδηγιών, η Ομάδα Συνεργασίας θα πρέπει να χαρτογραφεί με συνέπεια τις εθνικές λύσεις και εμπειρίες, να αξιολογεί τον αντίκτυπο των παραδοτέων της Ομάδας Συνεργασίας στις εθνικές προσεγγίσεις, να συζητά τις προκλήσεις εφαρμογής και να διατυπώνει ειδικές συστάσεις, ιδίως όσον αφορά τη διευκόλυνση της ευθυγράμμισης της μεταφοράς της παρούσας οδηγίας στο εθνικό δίκαιο των κρατών μελών, οι οποίες πρέπει να αντιμετωπιστούν μέσω της καλύτερης εφαρμογής των υφιστάμενων κανόνων. Η Ομάδα Συνεργασίας θα μπορούσε επίσης να χαρτογραφήσει τις εθνικές λύσεις, προκειμένου να προωθήσει τη συμβατότητα των λύσεων κυβερνοασφάλειας που εφαρμόζονται σε κάθε συγκεκριμένο τομέα σε ολόκληρη την Ένωση. Αυτό είναι ιδιαίτερα σημαντικό στους τομείς με διεθνή ή διασυνοριακό χαρακτήρα.

(66) Η Ομάδα Συνεργασίας θα πρέπει να παραμείνει ένα ευέλικτο φόρουμ και να είναι σε θέση να αντιδρά σε μεταβαλλόμενες και νέες πολιτικές προτεραιότητες και προκλήσεις, λαμβάνοντας παράλληλα υπόψη τη διαθεσιμότητα των πόρων. Θα μπορούσε να οργανώνει τακτικές κοινές συνεδριάσεις με σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που διεξάγονται από την Ομάδα Συνεργασίας και τη συλλογή δεδομένων και στοιχείων σχετικά με τις αναδυόμενες προκλήσεις πολιτικής. Επιπλέον, η Ομάδα Συνεργασίας θα πρέπει να διενεργεί τακτική αξιολόγηση της κατάστασης σε σχέση με κυβερνοαπειλές ή περιστατικά στον κυβερνοχώρο, όπως επιθέσεις λυτρισμικού. Προκειμένου να ενισχυθεί η συνεργασία σε επίπεδο Ένωσης, η Ομάδα Συνεργασίας θα πρέπει να εξετάσει το

ενδεχόμενο να καλέσει τα σχετικά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που μετέχουν στην πολιτική για την κυβερνοασφάλεια, όπως το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπόλ, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας, που συστάθηκε με τον κανονισμό (ΕΕ) 2018/1139, και τον Οργανισμό της Ευρωπαϊκής Ένωσης για το διαστημικό πρόγραμμα, που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/696 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14]), να συμμετάσχουν στις εργασίες της.

(67) Οι αρμόδιες αρχές και οι CSIRT θα πρέπει να μπορούν να συμμετέχουν σε προγράμματα ανταλλαγής υπαλλήλων από άλλα κράτη μέλη, εντός ειδικού πλαισίου και, κατά περίπτωση, με την επιφύλαξη της απαιτούμενης εξουσιοδότησης ασφαλείας των υπαλλήλων που συμμετέχουν στα εν λόγω συστήματα ανταλλαγής, προκειμένου να βελτιωθεί η συνεργασία και να ενισχυθεί η εμπιστοσύνη μεταξύ των κρατών μελών. Οι αρμόδιες αρχές θα πρέπει να λαμβάνουν τα αναγκαία μέτρα ώστε οι υπάλληλοι από άλλα κράτη μέλη να είναι σε θέση να συμμετέχουν αποτελεσματικά στις δραστηριότητες της φιλοξενούσας αρμόδιας αρχής ή της φιλοξενούσας CSIRT.

(68) Τα κράτη μέλη θα πρέπει να συμβάλουν στη δημιουργία του πλαισίου της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο που ορίζεται στη σύσταση (ΕΕ) 2017/1584 της Επιτροπής ([15]) μέσω των υφιστάμενων δικτύων συνεργασίας, ιδίως του του ευρωπαϊκού δικτύου οργανισμών διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe), του δικτύου CSIRT και της ομάδας συνεργασίας. Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να συνεργάζονται βάσει διαδικαστικών ρυθμίσεων που θα καθορίζουν τις λεπτομέρειες της εν λόγω συνεργασίας και να αποφεύγουν τυχόν αλληλοεπικάλυψη εργασιών. Οι διαδικαστικοί κανόνες του EU-CyCLONe θα πρέπει να προσδιορίζουν περαιτέρω τις ρυθμίσεις για τη λειτουργία του δικτύου, συμπεριλαμβανομένων των ρόλων, των τρόπων συνεργασίας, των αλληλεπιδράσεων του δικτύου με άλλους σχετικούς παράγοντες και των υποδειγμάτων για την ανταλλαγή πληροφοριών, καθώς και των μέσων επικοινωνίας. Για τη διαχείριση κρίσεων σε επίπεδο Ένωσης, τα ενδιαφερόμενα μέρη θα πρέπει να βασίζονται στις ολοκληρωμένες ρυθμίσεις της ΕΕ για την αντιμετώπιση πολιτικών κρίσεων δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 του Συμβουλίου ([16]) (ρυθμίσεις IPCR). Η Επιτροπή θα πρέπει να χρησιμοποιήσει για τον σκοπό αυτό την υψηλού επιπέδου διαδικασία ARGUS για τον συντονισμό σε περιπτώσεις διατομεακών κρίσεων. Εάν η κρίση ενέχει σημαντική εξωτερική διάσταση ή διάσταση κοινής πολιτικής ασφάλειας και άμυνας, θα πρέπει να ενεργοποιείται ο Μηχανισμός Αντιμετώπισης Κρίσεων της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης.

(69) Σύμφωνα με το παράρτημα της σύστασης (ΕΕ) 2017/1584, ως περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας θα πρέπει να νοείται εκείνο το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη. Ανάλογα με την αιτία και τις συνέπειές τους, τα περιστατικά μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας ενδέχεται να κλιμακωθούν και να μετατραπούν σε πραγματικές κρίσεις που καθιστούν αδύνατη την ομαλή λειτουργία της εσωτερικής αγοράς ή θέτουν σε σοβαρό κίνδυνο τη δημόσια ασφάλεια οντοτήτων ή πολιτών σε διάφορα κράτη μέλη ή την Ένωση στο σύνολό της. Δεδομένου των ευρειών συνεπειών και, στις περισσότερες περιπτώσεις, του διασυνοριακού χαρακτήρα τέτοιων περιστατικών, τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα πρέπει να συνεργάζονται σε τεχνικό, επιχειρησιακό και πολιτικό επίπεδο για τον κατάλληλο συντονισμό της αντιμετώπισής τους σε ολόκληρη την Ένωση.

(70) Τα περιστατικά μεγάλης κλίμακας και οι κρίσεις στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης απαιτούν συντονισμένη δράση για τη διασφάλιση ταχείας και αποτελεσματικής αντίδρασης, λόγω του υψηλού βαθμού αλληλεξάρτησης μεταξύ τομέων και κρατών μελών. Η διαθεσιμότητα κυβερνοανθεκτικών συστημάτων δικτύων και πληροφοριών και η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι ζωτικής σημασίας για την ασφάλεια της Ένωσης και για την προστασία των πολιτών, των επιχειρήσεων και των θεσμικών οργάνων της από περιστατικά και κυβερνοαπειλές, καθώς και για την ενίσχυση της εμπιστοσύνης των ατόμων και των οργανισμών στην ικανότητα της Ένωσης να προωθεί και να προστατεύει έναν παγκόσμιο, ανοικτό, ελεύθερο, σταθερό και ασφαλή κυβερνοχώρο που θα βασίζεται στα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες, τη δημοκρατία και το κράτος δικαίου.

([14]) Κανονισμός (ΕΕ) 2021/696 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Απριλίου 2021, για τη θέσπιση του ενωσιακού διαστημικού προγράμματος και του Οργανισμού της Ευρωπαϊκής Ένωσης για το διαστημικό πρόγραμμα, και για την κατάργηση των κανονισμών (ΕΕ) αριθ. 912/2010, (ΕΕ) αριθ. 1285/2013 και (ΕΕ) αριθ. 377/2014 και της απόφασης αριθ. 541/2014/ΕΕ (ΕΕ L 170 της 12.5.2021, σ. 69).

([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).

([16]) Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ (ΕΕ L 320 της 17.12.2018, σ. 28).

(71) Το EU-CyCLONe θα πρέπει να λειτουργεί ως ενδιάμεσος μεταξύ του τεχνικού και του πολιτικού επιπέδου κατά τη διάρκεια περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, να ενισχύει τη συνεργασία σε επιχειρησιακό επίπεδο και να στηρίζει τη λήψη αποφάσεων σε πολιτικό επίπεδο. Σε συνεργασία με την Επιτροπή, έχοντας υπόψη την αρμοδιότητα της Επιτροπής στον τομέα της διαχείρισης κρίσεων, το EU-CyCLONe θα πρέπει να αξιοποιεί τα πορίσματα του δικτύου CSIRT και να χρησιμοποιεί τις δικές του ικανότητες για τη δημιουργία ανάλυσης επιπτώσεων περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας.

(72) Οι κυβερνοεπιθέσεις έχουν διασυνοριακό χαρακτήρα και ένα σημαντικό περιστατικό μπορεί να διαταράξει και να βλάψει κρίσιμες υποδομές πληροφοριών από τις οποίες εξαρτάται η ομαλή λειτουργία της εσωτερικής αγοράς. Η σύσταση (ΕΕ) 2017/1584 προσδιορίζει τον ρόλο όλων των σχετικών φορέων. Επιπλέον, η Επιτροπή είναι υπεύθυνη, στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης που θεσπίστηκε με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17]), για γενικές δράσεις ετοιμότητας, συμπεριλαμβανομένης της διαχείρισης του Κέντρου Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών και του Κοινού Συστήματος Επικοινωνίας και Πληροφόρησης Έκτακτης Ανάγκης, για τη διατήρηση και περαιτέρω ανάπτυξη ικανοτήτων επίγνωσης και ανάλυσης της κατάστασης, και για τη δημιουργία και διαχείριση της ικανότητας κινητοποίησης και αποστολής ομάδων εμπειρογνωμόνων σε περίπτωση αιτήματος παροχής βοήθειας από κράτος μέλος ή τρίτη χώρα. Η Επιτροπή είναι επίσης αρμόδια για την υποβολή αναλυτικών εκθέσεων σχετικά με τις ρυθμίσεις IPCR δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993, μεταξύ άλλων σε σχέση με την επίγνωση της κατάστασης και την ετοιμότητα στον τομέα της κυβερνοασφάλειας, καθώς και για την επίγνωση της κατάστασης και την αντιμετώπιση κρίσεων στους τομείς της γεωργίας, των δυσμενών καιρικών συνθηκών, της χαρτογράφησης και των προβλέψεων συγκρούσεων, των συστημάτων έγκαιρης προειδοποίησης για φυσικές καταστροφές, των καταστάσεων έκτακτης ανάγκης στον τομέα της υγείας, της επιτήρησης λοιμώξεων, της υγείας των φυτών, των περιστατικών χημικής ασφάλειας, της ασφάλειας των τροφίμων και των ζωοτροφών, της υγείας των ζώων, της μετανάστευσης, των τελωνείων, των καταστάσεων έκτακτης ανάγκης στον τομέα της πυρηνικής και ραδιολογικής κατάστασης, και της ενέργειας.

(73) Η Ένωση μπορεί, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς, που επιτρέπουν και οργανώνουν τη συμμετοχή τους σε ορισμένες δραστηριότητες της Ομάδας Συνεργασίας και του δικτύου CSIRT και EU-CyCLONe. Οι συμφωνίες αυτές θα πρέπει να διασφαλίζουν τα συμφέροντα της Ένωσης και την επαρκή προστασία των δεδομένων. Αυτό δεν θα πρέπει να αποκλείει το δικαίωμα των κρατών μελών να συνεργάζονται με τρίτες χώρες για τη διαχείριση τρωτοτήτων και τη διαχείριση κινδύνων κυβερνοασφάλειας, διευκολύνοντας την κοινοποίηση και τη γενική ανταλλαγή πληροφοριών σύμφωνα με το δίκαιο της Ένωσης.

(74) Προκειμένου να διευκολυνθεί η αποτελεσματική εφαρμογή της παρούσας οδηγίας όσον αφορά, μεταξύ άλλων, τη διαχείριση τρωτοτήτων, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, τις υποχρεώσεις κοινοποίησης και τις ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη μπορούν να συνεργάζονται με τρίτες χώρες και να αναλαμβάνουν δραστηριότητες που θεωρούνται κατάλληλες για τον σκοπό αυτό, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών σχετικά με κυβερνοαπειλές, περιστατικά, τρωτότητες, εργαλεία και μεθόδους, τακτικές, τεχνικές και διαδικασίες, ετοιμότητα και ασκήσεις διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας, κατάρτιση, οικοδόμηση εμπιστοσύνης και ρυθμίσεις για διαρθρωμένη ανταλλαγή πληροφοριών.

(75) Θα πρέπει να εισαχθούν αξιολογήσεις από ομοτίμους για να διευκολυνθεί η άντληση διδαγμάτων από τις κοινές εμπειρίες, να ενισχυθεί η αμοιβαία εμπιστοσύνη και να επιτευχθεί υψηλό κοινό επίπεδο κυβερνοασφάλειας. Οι αξιολογήσεις από ομοτίμους μπορούν να οδηγήσουν σε πολύτιμες πληροφορίες και συστάσεις που ενισχύουν τις συνολικές ικανότητες κυβερνοασφάλειας, δημιουργώντας μια ακόμη λειτουργική οδό για την ανταλλαγή βέλτιστων πρακτικών μεταξύ των κρατών μελών και συμβάλλοντας στην ενίσχυση των επιπέδων ωριμότητας των κρατών μελών στον τομέα της κυβερνοασφάλειας. Επιπλέον, οι αξιολογήσεις από ομοτίμους θα πρέπει να λαμβάνουν υπόψη τα αποτελέσματα παρόμοιων μηχανισμών, όπως το σύστημα αξιολόγησης από ομοτίμους του δικτύου CSIRT, και θα πρέπει να προσθέτουν αξία και να αποφεύγουν τις επικαλύψεις. Η εφαρμογή των αξιολογήσεων από ομοτίμους δεν θα πρέπει να θίγει το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία των εμπιστευτικών ή διαβαθμισμένων πληροφοριών.

(76) Η Ομάδα Συνεργασίας θα πρέπει να θεσπίσει μεθοδολογία αυτοαξιολόγησης για τα κράτη μέλη, με στόχο την κάλυψη παραγόντων όπως το επίπεδο εφαρμογής των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων, το επίπεδο ικανοτήτων και η αποτελεσματικότητα της άσκησης των καθηκόντων των αρμόδιων αρχών, οι επιχειρησιακές ικανότητες των CSIRT, το επίπεδο εφαρμογής της αμοιβαίας συνδρομής, το επίπεδο εφαρμογής των ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας ή ειδικά ζητήματα διασυνοριακού ή διατομεακού χαρακτήρα. Τα κράτη μέλη θα πρέπει να ενθαρρύνονται να διενεργούν αυτοαξιολογήσεις σε τακτική βάση, καθώς και να παρουσιάζουν και να συζητούν τα αποτελέσματα της αυτοαξιολόγησής τους στο πλαίσιο της Ομάδας Συνεργασίας.

([17]) Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

(77) Η ευθύνη για την εξασφάλιση της ασφάλειας των συστημάτων δικτύου και πληροφοριών εναπόκειται σε μεγάλο βαθμό στις βασικές και στις σημαντικές οντότητες. Θα πρέπει να προωθηθεί και να αναπτυχθεί μια αντίληψη διαχείρισης κινδύνων η οποία θα περιλαμβάνει εκτιμήσεις κινδύνου και την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας κατάλληλα για τους αντιμετωπιζόμενους κινδύνους.

(78) Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να λαμβάνουν υπόψη τον βαθμό εξάρτησης της βασικής ή σημαντικής οντότητας από τα συστήματα δικτύου και πληροφοριών και να περιλαμβάνουν μέτρα για τον εντοπισμό τυχόν κινδύνων περιστατικών, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση περιστατικών και την ανάκαμψη από αυτά, καθώς και για τον μετριασμό των επιπτώσεών τους. Η ασφάλεια των συστημάτων δικτύου και πληροφοριών θα πρέπει να περιλαμβάνει την ασφάλεια των αποθηκευμένων, διαβιβαζόμενων και υφιστάμενων σε επεξεργασία δεδομένων. Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να προβλέπουν συστημική ανάλυση, λαμβάνοντας υπόψη τον ανθρώπινο παράγοντα, προκειμένου να υπάρχει πλήρης εικόνα της ασφάλειας του συστήματος δικτύου και πληροφοριών.

(79) Δεδομένου ότι οι απειλές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών μπορεί να έχουν διαφορετικές προελεύσεις, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να βασίζονται σε μια ολική προσέγγιση των κινδύνων, η οποία να αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά όπως κλοπή, πυρκαγιά, πλημμύρες, αστοχίες στις τηλεπικοινωνίες ή την ηλεκτροδότηση, ή η μη εξουσιοδοτημένη φυσική πρόσβαση, καταστροφή και παρέμβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών της βασικής ή σημαντικής οντότητας, οι οποίες θα μπορούσαν να θέσουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών. Συνεπώς, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει επίσης να αφορούν τη φυσική και περιβαλλοντική ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβάνοντας μέτρα για την προστασία των εν λόγω συστημάτων από αστοχίες του συστήματος, ανθρώπινα σφάλματα, κακόβουλες πράξεις ή φυσικά φαινόμενα, σύμφωνα με τα ευρωπαϊκά και διεθνή πρότυπα, όπως αυτά που περιλαμβάνονται στη σειρά ISO/IEC 27000. Εν προκειμένω, οι βασικές και σημαντικές οντότητες θα πρέπει, στο πλαίσιο των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που εφαρμόζουν, να μεριμνούν και για την ασφάλεια των ανθρώπινων πόρων και να εφαρμόζουν κατάλληλες πολιτικές ελέγχου της πρόσβασης. Τα μέτρα αυτά θα πρέπει να συνάδουν με την οδηγία (ΕΕ) 2022/2557.

(80) Για τον σκοπό της απόδειξης της συμμόρφωσης με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και ελλείψει κατάλληλων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που να έχουν εγκριθεί σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]), τα κράτη μέλη θα πρέπει, σε διαβούλευση με την Ομάδα Συνεργασίας και την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, να προωθούν τη χρήση σχετικών ευρωπαϊκών και διεθνών προτύπων από βασικές και σημαντικές οντότητες ή να απαιτούν από οντότητες να χρησιμοποιούν πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ.

(81) Προκειμένου να αποφευχθεί η επιβολή δυσανάλογης οικονομικής και διοικητικής επιβάρυνσης σε βασικές και σημαντικές οντότητες, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι αναλογικά προς τους κινδύνους που εγκυμονεί το οικείο σύστημα δικτύου και πληροφοριών, λαμβάνοντας υπόψη την πλέον προηγμένη τεχνολογία των εν λόγω μέτρων και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, καθώς και το κόστος εφαρμογής τους.

(82) Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι αναλογικά προς τον βαθμό έκθεσης της βασικής ή σημαντικής οντότητας σε κινδύνους και προς τον κοινωνικό και οικονομικό αντίκτυπο που θα είχε ένα περιστατικό. Κατά τη θέσπιση μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, προσαρμοσμένων στις βασικές και σημαντικές οντότητες, θα πρέπει να λαμβάνονται δεόντως υπόψη ο διαφορετικός βαθμός έκθεσης στον κίνδυνο για τις βασικές και σημαντικές οντότητες, όπως η κρισιμότητα της οντότητας, οι κίνδυνοι, συμπεριλαμβανομένων των κοινωνικών κινδύνων στους οποίους είναι εκτεθειμένη, το μέγεθος της οντότητας και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους.

([18]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

(83) Οι βασικές και οι σημαντικές οντότητες θα πρέπει να εγγυώνται την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους. Τα συστήματα αυτά είναι κυρίως ιδιωτικά συστήματα δικτύου και πληροφοριών τα οποία διαχειρίζεται το εσωτερικό προσωπικό ΤΠ των βασικών και σημαντικών οντοτήτων ή των οποίων η ασφάλεια έχει ανατεθεί σε εξωτερικούς συνεργάτες. Τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και οι υποχρεώσεις υποβολής εκθέσεων που προβλέπονται στην παρούσα οδηγία θα πρέπει να εφαρμόζονται στις σχετικές βασικές και σημαντικές οντότητες, ανεξάρτητα από το αν οι εν λόγω οντότητες διατηρούν εσωτερικά τα συστήματα δικτύου και πληροφοριών τους ή αναθέτουν τη συντήρησή τους σε εξωτερικούς συνεργάτες.

(84) Λαμβανομένου υπόψη του διασυνοριακού χαρακτήρα τους, οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD, οι πάροχοι υπηρεσιών υπολογιστικού νέφους, οι πάροχοι υπηρεσιών κέντρων δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι υπηρεσιών υπό διαχείριση, οι πάροχοι υπηρεσιών ασφάλειας υπό διαχείριση, οι πάροχοι επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης και οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υπόκεινται σε υψηλό βαθμό εναρμόνισης σε επίπεδο Ένωσης. Κατά συνέπεια, η εφαρμογή των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας όσον αφορά τις εν λόγω οντότητες θα πρέπει να διευκολυνθεί με εκτελεστική πράξη.

(85) Η αντιμετώπιση των κινδύνων που απορρέουν από την αλυσίδα εφοδιασμού μιας οντότητας και τη σχέση της με τους προμηθευτές της, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή οι πάροχοι διαχειριζόμενης υπηρεσίας ασφάλειας και οι εκδότες λογισμικού, είναι ιδιαίτερα σημαντική δεδομένης της επικράτησης περιστατικών κατά τα οποία οντότητες έχουν πέσει θύματα κυβερνοεπιθέσεων και όπου κακόβουλοι δράστες μπόρεσαν να θέσουν σε κίνδυνο την ασφάλεια των συστημάτων δικτύου και πληροφοριών μιας οντότητας εκμεταλλευόμενοι ευπάθειες προϊόντων και υπηρεσιών τρίτων. Επομένως, οι βασικές και σημαντικές οντότητες θα πρέπει να αξιολογούν και να λαμβάνουν υπόψη τη συνολική ποιότητα και ανθεκτικότητα των προϊόντων και των υπηρεσιών, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ενσωματώνονται σε αυτά, καθώς και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους. Οι βασικές και σημαντικές οντότητες θα πρέπει ιδίως να ενθαρρύνονται να ενσωματώνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας στις συμβατικές ρυθμίσεις με τους άμεσους προμηθευτές και τους παρόχους υπηρεσιών τους. Οι εν λόγω οντότητες θα μπορούσαν να εξετάζουν τους κινδύνους που απορρέουν από άλλα επίπεδα προμηθευτών και παρόχων υπηρεσιών.

(86) Μεταξύ των παρόχων υπηρεσιών, οι πάροχοι υπηρεσίας διαχείρισης της ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στην παροχή συνδρομής σε οντότητες που καταβάλλουν προσπάθειες για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών ή την ανάκαμψη από αυτά. Ωστόσο, οι ίδιοι οι πάροχοι υπηρεσίας ασφάλειας που τελούν υπό διαχείριση αποτέλεσαν επίσης στόχο κυβερνοεπιθέσεων και, λόγω της στενής ενσωμάτωσής τους στη λειτουργία των οντοτήτων, εγκυμονούν ιδιαίτερο κίνδυνο. Συνεπώς, οι βασικές και σημαντικές οντότητες θα πρέπει να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή παρόχου διαχειριζόμενης υπηρεσίας ασφάλειας.

(87) Οι αρμόδιες αρχές, στο πλαίσιο των εποπτικών καθηκόντων τους, μπορούν επίσης να επωφελούνται από υπηρεσίες κυβερνοασφάλειας, όπως οι έλεγχοι ασφάλειας και οι δοκιμές διείσδυσης ή η αντιμετώπιση περιστατικών.

(88) Οι βασικές και σημαντικές οντότητες θα πρέπει επίσης να αντιμετωπίζουν τους κινδύνους που απορρέουν από τις αλληλεπιδράσεις και τις σχέσεις τους με άλλα ενδιαφερόμενα μέρη εντός ενός ευρύτερου οικοσυστήματος, μεταξύ άλλων όσον αφορά την αντιμετώπιση της βιομηχανικής κατασκοπείας και την προστασία του εμπορικού απορρήτου. Ειδικότερα, οι εν λόγω οντότητες θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ώστε η συνεργασία τους με ακαδημαϊκά και ερευνητικά ιδρύματα να πραγματοποιείται σύμφωνα με τις πολιτικές τους για την κυβερνοασφάλεια και να ακολουθεί τις ορθές πρακτικές όσον αφορά την ασφαλή πρόσβαση και διάδοση των πληροφοριών εν γένει και την προστασία της πνευματικής ιδιοκτησίας ειδικότερα. Ομοίως, δεδομένης της σημασίας και της αξίας που έχουν τα δεδομένα για τις δραστηριότητες των βασικών και σημαντικών οντοτήτων, όταν βασίζονται σε υπηρεσίες μετασχηματισμού και ανάλυσης δεδομένων από τρίτα μέρη, οι εν λόγω οντότητες θα πρέπει να λαμβάνουν όλα τα κατάλληλα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.

(89) Οι βασικές και σημαντικές οντότητες θα πρέπει να υιοθετήσουν ένα ευρύ φάσμα βασικών πρακτικών κυβερνοϋγιεινής, όπως τις αρχές μηδενικής εμπιστοσύνης, αναβαθμίσεις λογισμικού, παραμετροποίηση ρυθμίσεων συσκευών, κατάτμηση δικτύου, ταυτοποίηση και διαχείριση πρόσβασης ή ευαισθητοποίηση του χρήστη, να οργανώνουν προγράμματα κατάρτισης για το προσωπικό τους και να λαμβάνουν μέτρα ευαισθητοποίησης σχετικά με κυβερνοαπειλές μέσω εταιρικού ηλεκτρονικού ταχυδρομείου, ηλεκτρονικού «ψαρέματος» ή τεχνικών κοινωνικής μηχανικής. Επιπλέον, οι εν λόγω οντότητες θα πρέπει να αξιολογούν τις δικές τους ικανότητες κυβερνοασφάλειας και, κατά περίπτωση, να επιδιώκουν την ενσωμάτωση τεχνολογιών που ενισχύουν την κυβερνοασφάλεια, όπως η τεχνητή νοημοσύνη ή τα συστήματα μηχανικής μάθησης, για την ενίσχυση των ικανοτήτων τους και της ασφάλειας των συστημάτων δικτύου και πληροφοριών.

(90) Για την περαιτέρω αντιμετώπιση των βασικών κινδύνων της αλυσίδας εφοδιασμού και την παροχή βοήθειας σε βασικές και σημαντικές οντότητες που δραστηριοποιούνται σε τομείς που καλύπτονται από την παρούσα οδηγία για την κατάλληλη διαχείριση των κινδύνων που σχετίζονται με την αλυσίδα εφοδιασμού και τους προμηθευτές, η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, και, κατά περίπτωση, κατόπιν διαβούλευσης με τα σχετικά ενδιαφερόμενα μέρη, μεταξύ άλλων από τη βιομηχανία, θα πρέπει να διενεργεί συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού, όπως διενεργούνται για τα δίκτυα 5G σύμφωνα με τη σύσταση (ΕΕ) 2019/534 της Επιτροπής ([19]), με σκοπό τον προσδιορισμό, ανά τομέα, των κρίσιμων υπηρεσιών ΤΠΕ, των συστημάτων ΤΠΕ ή των προϊόντων ΤΠΕ, των σχετικών απειλών και ευπαθειών. Οι εν λόγω συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια θα πρέπει να προσδιορίζουν μέτρα, σχέδια μετριασμού και βέλτιστες πρακτικές για την αντιμετώπιση κρίσιμων εξαρτήσεων, πιθανών μεμονωμένων σημείων αστοχίας, απειλών, τρωτοτήτων και άλλων κινδύνων που συνδέονται με την αλυσίδα εφοδιασμού και θα πρέπει να διερευνούν τρόπους για την περαιτέρω ενθάρρυνση της ευρύτερης υιοθέτησής τους από τις βασικές και σημαντικές οντότητες. Πιθανοί μη τεχνικοί παράγοντες κινδύνου, όπως η αθέμιτη επιρροή τρίτης χώρας στους προμηθευτές και τους παρόχους υπηρεσιών, ιδίως στην περίπτωση εναλλακτικών μοντέλων διακυβέρνησης, ενέχουν κεκαλυμμένες ευπάθειες ή κερκόπορτες και δυνητικές συστημικές διαταραχές στον εφοδιασμό, ιδίως σε περίπτωση τεχνολογικού εγκλωβισμού ή εξάρτησης από παρόχους.

(91) Οι συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού, υπό το φως των χαρακτηριστικών του οικείου τομέα, θα πρέπει να λαμβάνουν υπόψη τόσο τεχνικούς όσο και, κατά περίπτωση, μη τεχνικούς παράγοντες, συμπεριλαμβανομένων εκείνων που ορίζονται στη σύσταση (ΕΕ) 2019/534, στην πανευρωπαϊκή συντονισμένη εκτίμηση κινδύνου της ασφάλειας των δικτύων 5G και στην εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G που συμφωνήθηκε από την Ομάδα Συνεργασίας. Ο προσδιορισμός των αλυσίδων εφοδιασμού που θα πρέπει να υποβάλλονται σε συντονισμένη εκτίμηση κινδύνου για την ασφάλεια θα πρέπει να γίνεται με γνώμονα τα ακόλουθα κριτήρια: i) τον βαθμό στον οποίο βασικές και σημαντικές οντότητες χρησιμοποιούν και βασίζονται σε συγκεκριμένες κρίσιμες υπηρεσίες ΤΠΕ, συστήματα ΤΠΕ ή προϊόντα ΤΠΕ· ii) τη σημασία συγκεκριμένων κρίσιμων υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, συμπεριλαμβανομένης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· iii) τη διαθεσιμότητα εναλλακτικών υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ· iv) την ανθεκτικότητα του συνόλου της αλυσίδας εφοδιασμού υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή προϊόντων ΤΠΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους έναντι γεγονότων που προκαλούν διατάραξη και v) όσον αφορά αναδυόμενες υπηρεσίες ΤΠΕ, συστήματα ΤΠΕ ή προϊόντα ΤΠΕ, τη δυνητική μελλοντική τους σημασία για τις δραστηριότητες των οντοτήτων. Επιπλέον, θα πρέπει να δοθεί ιδιαίτερη έμφαση στις υπηρεσίες ΤΠΕ, τα συστήματα ΤΠΕ ή τα προϊόντα ΤΠΕ που υπόκεινται σε ειδικές απαιτήσεις που απορρέουν από τρίτες χώρες.

(92) Προκειμένου να εξορθολογιστούν οι υποχρεώσεις που επιβάλλονται στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και στους παρόχους υπηρεσιών εμπιστοσύνης, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους, καθώς και να δοθεί η δυνατότητα στις εν λόγω οντότητες και στις αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]) και του κανονισμού (ΕΕ) αριθ. 910/2014 αντίστοιχα να επωφεληθούν από το νομικό πλαίσιο που θεσπίζεται με την παρούσα οδηγία, συμπεριλαμβανομένου του ορισμού μιας ομάδας CSIRT υπεύθυνης για τον χειρισμό περιστατικών, της συμμετοχής των οικείων αρμόδιων αρχών στις δραστηριότητες της ομάδας συνεργασίας και του δικτύου CSIRT, οι εν λόγω οντότητες θα πρέπει να υπάγονται στο πεδίο εφαρμογής της παρούσας οδηγίας. Συνεπώς, οι αντίστοιχες διατάξεις του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 σχετικά με την επιβολή απαιτήσεων ασφάλειας και κοινοποίησης σε αυτούς τους τύπους οντοτήτων, θα πρέπει να καταργηθούν. Οι κανόνες σχετικά με τις υποχρεώσεις υποβολής αναφορών που ορίζονται στην παρούσα οδηγία δεν θα πρέπει να θίγουν τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ.

(93) Οι υποχρεώσεις κυβερνοασφάλειας που ορίζονται στην παρούσα οδηγία θα πρέπει να θεωρούνται συμπληρωματικές προς τις απαιτήσεις που επιβάλλονται στους παρόχους υπηρεσιών εμπιστοσύνης δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014. Οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υποχρεούνται να λαμβάνουν όλα τα κατάλληλα και αναλογικά μέτρα για τη διαχείριση των πιθανών κινδύνων για τις υπηρεσίες τους, μεταξύ άλλων σε σχέση με τους πελάτες και τα βασιζόμενα τρίτα μέρη, και να αναφέρουν περιστατικά δυνάμει της παρούσας οδηγίας. Οι εν λόγω υποχρεώσεις κυβερνοασφάλειας και αναφοράς περιστατικών θα πρέπει να αφορούν και τη φυσική προστασία των παρεχόμενων υπηρεσιών. Οι απαιτήσεις για τους αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης που ορίζονται στο άρθρο 24 του κανονισμού (ΕΕ) αριθ. 910/2014 εξακολουθούν να ισχύουν.

([19]) Σύσταση (ΕΕ) 2019/534 της Επιτροπής, της 26ης Μαρτίου 2019, Κυβερνοασφάλεια δικτύων 5G (ΕΕ L 88 της 29.3.2019, σ. 42).

([20]) 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).

(94) Τα κράτη μέλη μπορούν να αναθέσουν τον ρόλο των αρμόδιων αρχών για τις υπηρεσίες εμπιστοσύνης στους εποπτικούς φορείς δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, προκειμένου να διασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που αποκτήθηκαν κατά την εφαρμογή του εν λόγω κανονισμού. Σε τέτοια περίπτωση, οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας, θα πρέπει να συνεργάζονται στενά και εγκαίρως με τους εν λόγω εποπτικούς φορείς, ανταλλάσσοντας τις σχετικές πληροφορίες, προκειμένου να εξασφαλίζεται η αποτελεσματική εποπτεία και συμμόρφωση των παρόχων υπηρεσιών εμπιστοσύνης με τις απαιτήσεις που ορίζονται στην παρούσα οδηγία και στον κανονισμό (ΕΕ) αριθ. 910/2014. Κατά περίπτωση, η CSIRT ή η αρμόδια αρχή δυνάμει της παρούσας οδηγίας θα πρέπει να ενημερώνει αμέσως τον εποπτικό φορέα δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με κάθε κοινοποιηθείσα σημαντική κυβερνοαπειλή ή περιστατικό με αντίκτυπο στις υπηρεσίες εμπιστοσύνης, καθώς και σχετικά με τυχόν παραβίασης της παρούσας οδηγίας εκ μέρους παρόχου υπηρεσιών εμπιστοσύνης. Για τους σκοπούς της κοινοποίησης, τα κράτη μέλη μπορούν να χρησιμοποιούν, κατά περίπτωση, το ενιαίο σημείο εισόδου που έχει θεσπιστεί για την επίτευξη κοινής και αυτόματης αναφοράς περιστατικών τόσο στον εποπτικό φορέα δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014 όσο και στην CSIRT ή στην αρμόδια αρχή δυνάμει της παρούσας οδηγίας.

(95) Κατά περίπτωση και προκειμένου να αποφευχθεί άσκοπη αναστάτωση, οι υφιστάμενες εθνικές κατευθυντήριες γραμμές που έχουν εγκριθεί για τη μεταφορά των κανόνων σχετικά με τα μέτρα ασφάλειας που προβλέπονται στα άρθρα 40 και 41 της οδηγίας (ΕΕ) 2018/1972, θα πρέπει να λαμβάνονται υπόψη κατά τη μεταφορά της παρούσας οδηγίας στο εθνικό δίκαιο, ώστε να αξιοποιηθούν οι γνώσεις και οι δεξιότητες που έχουν ήδη αποκτηθεί δυνάμει της οδηγίας (ΕΕ) 2018/1972 σχετικά με τα μέτρα ασφάλειας και τις κοινοποιήσεις περιστατικών. Ο ENISA μπορεί επίσης να καταρτίσει κατευθυντήριες γραμμές σχετικά με τις απαιτήσεις ασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών για τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να διευκολυνθούν η εναρμόνιση και η μετάβαση και να ελαχιστοποιηθούν οι διαταράξεις. Τα κράτη μέλη μπορούν να αναθέσουν στις εθνικές ρυθμιστικές αρχές τον ρόλο των αρμόδιων αρχών για τις ηλεκτρονικές επικοινωνίες δυνάμει της οδηγίας (ΕΕ) 2018/1972 προκειμένου να εξασφαλιστεί η συνέχιση των τρεχουσών πρακτικών και να αξιοποιηθούν οι γνώσεις και η πείρα που αποκτήθηκαν ως αποτέλεσμα της μεταφοράς της εν λόγω οδηγίας.

(96) Δεδομένης της αυξανόμενης σημασίας των υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού, όπως αυτές ορίζονται στην οδηγία (ΕΕ) 2018/1972, είναι αναγκαίο να εξασφαλίζεται ότι οι εν λόγω υπηρεσίες θα υπόκεινται επίσης σε κατάλληλες απαιτήσεις ασφάλειας σύμφωνα με τον συγκεκριμένο χαρακτήρα τους και την οικονομική τους σημασία. Καθώς η επιφάνεια επίθεσης συνεχίζει να επεκτείνεται, οι ανεξαρτήτως αριθμού υπηρεσίες διαπροσωπικών επικοινωνιών, όπως είναι οι υπηρεσίες ανταλλαγής μηνυμάτων, καθίστανται διαδεδομένοι φορείς επίθεσης. Οι κακόβουλοι δράστες χρησιμοποιούν πλατφόρμες για να επικοινωνούν με τα θύματα και να τα προσελκύουν να ανοίξουν παραβιασμένες ιστοσελίδες, με αποτέλεσμα να αυξάνεται η πιθανότητα περιστατικών που αφορούν στην εκμετάλλευση δεδομένων προσωπικού χαρακτήρα και, κατ' επέκταση, στην ασφάλεια των συστημάτων δικτύου και πληροφοριών. Οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού θα πρέπει να διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών κατάλληλο για τους κινδύνους που εγκυμονούν. Δεδομένου ότι οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμού κατά κανόνα δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων μέσω δικτύων, ο βαθμός κινδύνου για τις εν λόγω υπηρεσίες μπορεί να θεωρηθεί, από ορισμένες απόψεις, χαμηλότερος από ό,τι για τις παραδοσιακές υπηρεσίες ηλεκτρονικών επικοινωνιών. Το ίδιο ισχύει και για τις υπηρεσίες διαπροσωπικών επικοινωνιών όπως ορίζονται στην οδηγία (ΕΕ) 2018/1972 που χρησιμοποιούν αριθμούς και δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων.

(97) Η εσωτερική αγορά εξαρτάται περισσότερο από ποτέ από τη λειτουργία του διαδικτύου. Οι υπηρεσίες όλων, σχεδόν, των βασικών και των σημαντικών οντοτήτων εξαρτώνται από τις υπηρεσίες που παρέχονται μέσω του διαδικτύου. Προκειμένου να διασφαλιστεί η ομαλή παροχή υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες, είναι σημαντικό όλοι οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών να διαθέτουν κατάλληλα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και να αναφέρουν σχετικά σημαντικά περιστατικά. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι διατηρείται η ασφάλεια των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και ότι τα ζωτικά συμφέροντά τους στον τομέα της ασφάλειας προστατεύονται από δολιοφθορά και κατασκοπεία. Δεδομένου ότι η διεθνής συνδεσιμότητα ενισχύει και επιταχύνει την ανταγωνιστική ψηφιοποίηση της Ένωσης και της οικονομίας της, τα περιστατικά που επηρεάζουν τα υποβρύχια καλώδια επικοινωνιών θα πρέπει να αναφέρονται στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή. Η εθνική στρατηγική κυβερνοασφάλειας θα πρέπει, κατά περίπτωση, να λαμβάνει υπόψη την κυβερνοασφάλεια των υποθαλάσσιων καλωδίων επικοινωνιών και να περιλαμβάνει χαρτογράφηση των δυνητικών κινδύνων κυβερνοασφάλειας και μέτρα μετριασμού για τη διασφάλιση του υψηλότερου δυνατού επιπέδου προστασίας τους.

(98) Προκειμένου να προστατεύεται η ασφάλεια των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να προωθηθεί η χρήση τεχνολογιών κρυπτογράφησης, ιδίως διατερματικής κρυπτογράφησης, καθώς και εννοιών ασφάλειας με επίκεντρο τα δεδομένα, όπως χαρτογραφία, κατάτμηση, σήμανση, πολιτική πρόσβασης και διαχείριση πρόσβασης, καθώς και αποφάσεις αυτοματοποιημένης πρόσβασης. Όπου απαιτείται, η χρήση κρυπτογράφησης, ιδίως διατερματικής κρυπτογράφησης, θα πρέπει να είναι υποχρεωτική για τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σύμφωνα με τις αρχές της ασφάλειας και της ιδιωτικότητας εξ ορισμού και εκ σχεδιασμού για τους σκοπούς της παρούσας οδηγίας. Η χρήση της διατερματικής κρυπτογράφησης θα πρέπει να συμβιβάζεται με τις εξουσίες των κρατών μελών να διασφαλίζουν την προστασία των ουσιωδών συμφερόντων ασφάλειας και δημόσιας ασφάλειάς τους και να επιτρέπουν την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων σύμφωνα με το δίκαιο της Ένωσης. Ωστόσο, αυτό δεν θα πρέπει να αποδυναμώνει τη διατερματική κρυπτογράφηση, η οποία αποτελεί κρίσιμη τεχνολογία για την αποτελεσματική προστασία των δεδομένων, της ιδιωτικότητας και της ασφάλειας των επικοινωνιών.

(99) Προκειμένου να διαφυλαχθεί η ασφάλεια, και να αποτραπούν η κατάχρηση και η χειραγώγηση, των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, θα πρέπει να προωθηθεί η χρήση προτύπων ασφαλούς δρομολόγησης, ώστε να διασφαλιστεί η ακεραιότητα και η ευρωστία των λειτουργιών δρομολόγησης σε ολόκληρο το οικοσύστημα των παρόχων υπηρεσιών πρόσβασης στο διαδίκτυο.

(100) Προκειμένου να διασφαλιστούν η λειτουργικότητα και η ακεραιότητα του διαδικτύου και να προωθηθεί η ασφάλεια και η ανθεκτικότητα του DNS, τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των οντοτήτων του ιδιωτικού τομέα της Ένωσης, των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, ιδίως των παρόχων υπηρεσιών πρόσβασης στο διαδίκτυο και των παρόχων διαδικτυακών μηχανών αναζήτησης, θα πρέπει να ενθαρρυνθούν να υιοθετήσουν στρατηγική διαφοροποίησης της επίλυσης των ονομάτων DNS. Συνεπώς, τα κράτη μέλη θα πρέπει να ενθαρρύνουν την ανάπτυξη και χρήση μιας δημόσιας και ασφαλούς ευρωπαϊκής υπηρεσίας επίλυσης ονομάτων DNS.

(101) Η παρούσα οδηγία θεσπίζει μια προσέγγιση πολλαπλών σταδίων ως προς την αναφορά σοβαρών περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης σοβαρών περιστατικών και επιτρέπει στις βασικές και σημαντικές οντότητες να αναζητούν στήριξη και, αφετέρου, της υποβολής εμπεριστατωμένων εκθέσεων που αντλούν πολύτιμα διδάγματα από μεμονωμένα περιστατικά και βελτιώνουν με την πάροδο του χρόνου την κυβερνοανθεκτικότητα μεμονωμένων οντοτήτων και ολόκληρων τομέων. Στο πλαίσιο αυτό, η παρούσα οδηγία θα πρέπει να περιλαμβάνει την αναφορά περιστατικών τα οποία, βάσει αρχικής αξιολόγησης που διενεργείται από την οικεία οντότητα, θα μπορούσαν να προκαλέσουν σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία στην εν λόγω οντότητα ή να επηρεάσουν άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία. Στην εν λόγω αρχική αξιολόγηση θα πρέπει να λαμβάνονται υπόψη, μεταξύ άλλων, τα επηρεαζόμενα συστήματα δικτύου και πληροφοριών, και ιδίως η σημασία τους για την παροχή των υπηρεσιών της οντότητας, η σοβαρότητα και τα τεχνικά χαρακτηριστικά της κυβερνοαπειλής και τυχόν υποκείμενων τρωτοτήτων που αποτελούν αντικείμενο εκμετάλλευσης, καθώς και η πείρα της οντότητας σε παρόμοια περιστατικά. Δείκτες όπως ο βαθμός στον οποίο επηρεάζεται η λειτουργία της υπηρεσίας, η διάρκεια ενός περιστατικού ή ο αριθμός των επηρεαζόμενων αποδεκτών των υπηρεσιών θα μπορούσαν να διαδραματίσουν σημαντικό ρόλο στον προσδιορισμό του κατά πόσον η λειτουργική διατάραξη της υπηρεσίας είναι σοβαρή.

(102) Όταν οι βασικές και σημαντικές οντότητες αντιληφθούν σημαντικό περιστατικό, θα πρέπει να υποχρεούνται να υποβάλλουν έγκαιρη προειδοποίηση χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών. Η έγκαιρη προειδοποίηση θα πρέπει να ακολουθείται από κοινοποίηση περιστατικού. Οι οικείες οντότητες θα πρέπει να υποβάλλουν αμελλητί κοινοποίηση περιστατικού και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που αντιλαμβάνονται το σημαντικό περιστατικό, με σκοπό, ιδίως, την επικαιροποίηση των πληροφοριών που υποβάλλονται μέσω της έγκαιρης προειδοποίησης και την αναφορά αρχικής αξιολόγησης του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και ενδείξεων προσβολής, εφόσον υπάρχουν. Η τελική έκθεση θα πρέπει να υποβάλλεται το αργότερο ένα μήνα μετά την κοινοποίηση του περιστατικού. Η έγκαιρη προειδοποίηση θα πρέπει να περιλαμβάνει μόνο τις πληροφορίες που είναι αναγκαίες προκειμένου η CSIRT ή, κατά περίπτωση, η αρμόδια αρχή, να γνωρίζει το σημαντικό περιστατικό και να επιτρέπει στην οικεία οντότητα να ζητήσει βοήθεια, εφόσον απαιτείται. Η εν λόγω έγκαιρη προειδοποίηση, κατά περίπτωση, θα πρέπει να αναφέρει αν το σημαντικό περιστατικό είναι ύποπτο για έκνομες ή κακόβουλες πράξεις και αν είναι πιθανό να έχει διασυνοριακές επιπτώσεις. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι η υποχρέωση υποβολής της εν λόγω έγκαιρης προειδοποίησης, ή η επακόλουθη κοινοποίηση περιστατικών, δεν εκτρέπει τους πόρους της κοινοποιούσας οντότητας από δραστηριότητες που σχετίζονται με τον χειρισμό περιστατικών κατά προτεραιότητα, προκειμένου οι υποχρεώσεις αναφοράς περιστατικών να μην εκτρέπουν πόρους από τον χειρισμό

σημαντικών περιστατικών ή να θέτουν άλλως σε κίνδυνο τις σχετικές προσπάθειες της οντότητας. Σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι οικείες οντότητες υποβάλλουν έκθεση προόδου τη δεδομένη στιγμή και ότι έχει υποβληθεί τελική έκθεση εντός ενός μηνός από τον εκ μέρους τους χειρισμό του σημαντικού περιστατικού.

(103) Κατά περίπτωση, οι βασικές και σημαντικές οντότητες θα πρέπει να κοινοποιούν, χωρίς καθυστέρηση, στους αποδέκτες των υπηρεσιών τους τυχόν μέτρα ή διορθωτικά μέτρα που μπορούν να λάβουν για να μετριάσουν τους απορρέοντες κινδύνους από σημαντική κυβερνοαπειλή. Οι εν λόγω οντότητες θα πρέπει, κατά περίπτωση και ιδίως όταν η σημαντική κυβερνοαπειλή είναι πιθανό να συμβεί, να ενημερώνουν επίσης τους αποδέκτες των υπηρεσιών τους για την ίδια την απειλή. Η απαίτηση ενημέρωσης των αποδεκτών σημαντικών κυβερνοαπειλών θα πρέπει να τηρείται με τη μέγιστη δυνατή προσπάθεια, αλλά δεν θα πρέπει να απαλλάσσει τις εν λόγω οντότητες από την υποχρέωση να λαμβάνουν, με δικά τους έξοδα, κατάλληλα και άμεσα μέτρα για την πρόληψη ή την αντιμετώπιση τέτοιων απειλών και την αποκατάσταση του κανονικού επιπέδου ασφάλειας της υπηρεσίας. Η σχετική ενημέρωση προς τους αποδέκτες των υπηρεσιών σχετικά με σημαντικές κυβερνοαπειλές θα πρέπει να παρέχεται δωρεάν και να διατυπώνεται σε εύληπτη γλώσσα.

(104) Οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να εφαρμόζουν εκ σχεδιασμού και εξ ορισμού την ασφάλεια και να ενημερώνουν τους αποδέκτες των υπηρεσιών τους για σημαντικές κυβερνοαπειλές και για τα μέτρα που μπορούν να λάβουν για την προστασία της ασφάλειας των συσκευών και των επικοινωνιών τους, για παράδειγμα με τη χρήση ειδικών τύπων λογισμικού ή τεχνολογιών κρυπτογράφησης.

(105) Η προληπτική προσέγγιση των κυβερνοαπειλών αποτελεί ζωτικής σημασίας συνιστώσα των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, η οποία θα πρέπει να επιτρέπει στις αρμόδιες αρχές να αποτρέπουν αποτελεσματικά τη μετεξέλιξη κυβερνοαπειλών σε περιστατικά που ενδέχεται να προκαλέσουν σημαντική υλική ή μη υλική ζημία. Για τον σκοπό αυτό, η κοινοποίηση κυβερνοαπειλών έχει καθοριστική σημασία. Για τον σκοπό αυτό, οι οντότητες ενθαρρύνονται να αναφέρουν σε εθελοντική βάση τις κυβερνοαπειλές.

(106) Προκειμένου να απλουστευθεί η υποβολή των πληροφοριών που απαιτούνται βάσει της παρούσας οδηγίας, καθώς και να μειωθεί ο διοικητικός φόρτος για τις οντότητες, τα κράτη μέλη θα πρέπει να παρέχουν τεχνικά μέσα, όπως ενιαίο σημείο εισόδου, αυτοματοποιημένα συστήματα, διαδικτυακές φόρμες, φιλικές προς τον χρήστη διεπαφές, υποδείγματα, ειδικές πλατφόρμες για χρήση από οντότητες, ανεξαρτήτως του αν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, για την υποβολή των σχετικών πληροφοριών που πρέπει να αναφερθούν. Η ενωσιακή χρηματοδότηση για τη στήριξη της εφαρμογής της παρούσας οδηγίας, ιδίως στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21]), θα μπορούσε να περιλαμβάνει στήριξη για τα ενιαία σημεία εισόδου. Επιπλέον, οι οντότητες βρίσκονται συχνά αντιμέτωπες με καταστάσεις κατά τις οποίες ένα συγκεκριμένο περιστατικό, λόγω των χαρακτηριστικών του, πρέπει να αναφερθεί σε διαφορετικές αρχές, ως αποτέλεσμα των υποχρεώσεων κοινοποίησης που περιλαμβάνονται σε διάφορες νομικές πράξεις. Οι περιπτώσεις αυτές δημιουργούν πρόσθετο διοικητικό φόρτο και θα μπορούσαν επίσης να οδηγήσουν σε αβεβαιότητες όσον αφορά τη μορφή και τις διαδικασίες των εν λόγω κοινοποιήσεων. Όταν δημιουργείται ενιαίο σημείο εισόδου, τα κράτη μέλη ενθαρρύνονται επίσης να χρησιμοποιούν το εν λόγω ενιαίο σημείο εισόδου για κοινοποιήσεις περιστατικών ασφάλειας που απαιτούνται βάσει άλλης ενωσιακής νομοθεσίας, όπως ο κανονισμός (ΕΕ) 2016/679 και η οδηγία 2002/58/ΕΚ. Η χρήση του εν λόγω ενιαίου σημείου εισόδου για την αναφορά περιστατικών ασφάλειας βάσει του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ δεν θα πρέπει να επηρεάζει την εφαρμογή των διατάξεων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας 2002/58/ΕΚ, ιδίως εκείνων που αφορούν την ανεξαρτησία των αρχών που αναφέρονται σε αυτά. Ο ENISA, σε συνεργασία με την Ομάδα Συνεργασίας, θα πρέπει να αναπτύξει κοινά υποδείγματα κοινοποίησης μέσω κατευθυντήριων γραμμών για την απλούστευση και τον εξορθολογισμό των πληροφοριών που πρέπει να αναφερθούν δυνάμει του δικαίου της Ένωσης και τη μείωση του διοικητικού φόρτου των κοινοποιουσών οντοτήτων.

(107) Όταν υπάρχει υπόνοια ότι ένα περιστατικό σχετίζεται με σοβαρές εγκληματικές δραστηριότητες δυνάμει ενωσιακής ή εθνικής νομοθεσίας, τα κράτη μέλη θα πρέπει να παροτρύνουν τις βασικές και τις σημαντικές οντότητες με βάση τους ισχύοντες στο ενωσιακό δίκαιο κανόνες ποινικών διαδικασιών, να αναφέρουν περιστατικά εικαζόμενης σοβαρής εγκληματικής φύσεως στις αρμόδιες αρχές επιβολής του νόμου. Κατά περίπτωση, και με την επιφύλαξη των κανόνων προστασίας των δεδομένων προσωπικού χαρακτήρα που ισχύουν για την Ευρωπόλ, είναι επιθυμητό ο συντονισμός μεταξύ των αρμόδιων αρχών και των αρχών επιβολής του νόμου των διαφόρων κρατών μελών να διευκολύνεται από το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα (EC3), και από τον ENISA.

([21]) Κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη και την κατάργηση της απόφασης (ΕΕ) 2015/2240 (ΕΕ L 166 της 11.5.2021, σ. 1).

(108) Ως αποτέλεσμα περιστατικών, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες σχετικά με όλα τα σχετικά θέματα με τις αρχές που αναφέρονται στον κανονισμό (ΕΕ) 2016/679 και στην οδηγία 2002/58/ΕΚ.

(109) Η διατήρηση επακριβών και πλήρων βάσεων δεδομένων για δεδομένα καταχώρισης ονομάτων τομέα (τα λεγόμενα «δεδομένα WHOIS») και η παροχή νόμιμης πρόσβασης στα εν λόγω δεδομένα είναι ουσιαστικής σημασίας για τη διασφάλιση της ασφάλειας, της σταθερότητας και της ανθεκτικότητας του DNS, γεγονός που με τη σειρά του συμβάλλει σε υψηλό κοινό επίπεδο κυβερνοασφάλειας εντός της Ένωσης. Για τον συγκεκριμένο σκοπό, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να επεξεργάζονται ορισμένα δεδομένα που είναι αναγκαία για την επίτευξη του εν λόγω σκοπού. Η εν λόγω επεξεργασία θα πρέπει να συνιστά νομική υποχρέωση κατά την έννοια του άρθρου 6 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679. Η υποχρέωση αυτή δεν θίγει τη δυνατότητα συλλογής δεδομένων καταχώρισης ονομάτων τομέα για άλλους σκοπούς, για παράδειγμα βάσει συμβατικών ρυθμίσεων ή νομικών απαιτήσεων που καθορίζονται σε άλλο ενωσιακό ή εθνικό δίκαιο. Η υποχρέωση αυτή αποσκοπεί στην επίτευξη ενός πλήρους και ακριβούς συνόλου δεδομένων καταχώρισης και δεν θα πρέπει να έχει ως αποτέλεσμα την επανειλημμένη συλλογή των ίδιων δεδομένων. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να συνεργάζονται μεταξύ τους προκειμένου να αποφεύγεται η αλληλεπικάλυψη του εν λόγω καθήκοντος.

(110) Η διαθεσιμότητα και η έγκαιρη προσβασιμότητα των δεδομένων καταχώρισης ονομάτων τομέα στους νομίμως αιτούντες πρόσβαση είναι ουσιαστικής σημασίας για την πρόληψη και την καταπολέμηση της κατάχρησης του DNS, καθώς και για την πρόληψη και τον εντοπισμό και την αντιμετώπιση περιστατικών. Ως νομίμως αιτούντες πρόσβαση νοούνται τα φυσικά ή νομικά πρόσωπα που υποβάλλουν αίτηση βάσει του ενωσιακού ή του εθνικού δικαίου. Μπορούν να περιλαμβάνονται αρχές που είναι αρμόδιες δυνάμει της παρούσας οδηγίας και αρχές που είναι αρμόδιες δυνάμει του ενωσιακού ή του εθνικού δικαίου για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων, καθώς και CERT ή CSIRT. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να επιτρέπουν τη νόμιμη πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα, τα οποία είναι αναγκαία για τους σκοπούς του αιτήματος πρόσβασης, σε νομίμως αιτούντες πρόσβαση σύμφωνα με το ενωσιακό και το εθνικό δίκαιο. Το αίτημα των νομίμως αιτούντων πρόσβαση θα πρέπει να συνοδεύεται από αιτιολόγηση που να επιτρέπει την αξιολόγηση της αναγκαιότητας πρόσβασης στα δεδομένα.

(111) Προκειμένου να διασφαλιστεί η διαθεσιμότητα ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων χώρου, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων χώρου θα πρέπει να συλλέγουν και να εγγυώνται την ακεραιότητα και τη διαθεσιμότητα των δεδομένων καταχώρισης ονομάτων χώρου. Ειδικότερα, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη συλλογή και τη διατήρηση ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων τομέα, καθώς και για την πρόληψη και διόρθωση ανακριβών δεδομένων καταχώρισης σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να λαμβάνουν υπόψη, στο μέτρο του δυνατού, τα πρότυπα που αναπτύσσονται από τις πολυσυμμετοχικές δομές διακυβέρνησης σε διεθνές επίπεδο. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να καθιερώσουν και να εφαρμόζουν αναλογικές διαδικασίες για την επαλήθευση των δεδομένων καταχώρισης ονομάτων τομέα. Οι διαδικασίες αυτές θα πρέπει να αντικατοπτρίζουν τις βέλτιστες πρακτικές που χρησιμοποιούνται στον κλάδο και, στο μέτρο του δυνατού, την πρόοδο που έχει σημειωθεί στον τομέα της ηλεκτρονικής ταυτοποίησης. Παραδείγματα διαδικασιών επαλήθευσης μπορεί να είναι οι προληπτικοί που διενεργούνται κατά την καταχώριση και οι κατασταλτικοί έλεγχοι που διενεργούνται μετά την καταχώριση. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει, ιδίως, να επαληθεύουν τουλάχιστον ένα στοιχείο επικοινωνίας του καταχωρίζοντος.

(112) Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να υποχρεούνται να δημοσιοποιούν δεδομένα καταχώρισης ονομάτων τομέα που δεν εμπίπτουν στο πεδίο εφαρμογής της ενωσιακής νομοθεσίας για την προστασία των δεδομένων, όπως δεδομένα που αφορούν νομικά πρόσωπα, σύμφωνα με το προοίμιο του κανονισμού (ΕΕ) 2016/679. Για τα νομικά πρόσωπα, τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να δημοσιοποιούν τουλάχιστον το όνομα του καταχωρίζοντος και τον αριθμό τηλεφώνου επικοινωνίας. Η διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας θα πρέπει επίσης να δημοσιεύεται υπό την προϋπόθεση ότι δεν περιέχει δεδομένα προσωπικού χαρακτήρα, όπως ψευδώνυμα ηλεκτρονικού ταχυδρομείου ή λογαριασμούς υπηρεσίας. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει επίσης να καθιστούν δυνατή τη νόμιμη πρόσβαση από νομίμως αιτούντες πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα που αφορούν φυσικά πρόσωπα, σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη θα πρέπει να απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να απαντούν χωρίς αδικαιολόγητη καθυστέρηση σε αιτήματα γνωστοποίησης δεδομένων καταχώρισης ονομάτων τομέα από νομίμως αιτούντες πρόσβαση. Τα μητρώα ονομάτων TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη δημοσίευση και γνωστοποίηση δεδομένων καταχώρισης, συμπεριλαμβανομένων συμφωνιών

σε επίπεδο υπηρεσιών για την αντιμετώπιση αιτημάτων πρόσβασης από νομίμως αιτούντες πρόσβαση. Οι εν λόγω πολιτικές και διαδικασίες θα πρέπει να λαμβάνουν υπόψη, στο μέτρο του δυνατού, τυχόν κατευθύνσεις που έχουν δοθεί καθώς και τα πρότυπα που αναπτύσσονται από τις πολυσυμμετοχικές δομές διακυβέρνησης σε διεθνές επίπεδο. Η διαδικασία πρόσβασης θα μπορούσε να περιλαμβάνει τη χρήση διεπαφής, πύλης ή άλλου τεχνικού εργαλείου για την παροχή αποτελεσματικού συστήματος υποβολής αιτημάτων για δεδομένα καταχώρισης και την πρόσβαση σε αυτά. Για την προώθηση εναρμονισμένων πρακτικών σε ολόκληρη την εσωτερική αγορά, η Επιτροπή μπορεί, με την επιφύλαξη των αρμοδιοτήτων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, να προβλέπει κατευθυντήριες γραμμές σχετικά με τις εν λόγω διαδικασίες, οι οποίες λαμβάνουν υπόψη, στο μέτρο του δυνατού, τα πρότυπα που έχουν αναπτυχθεί από τις πολυμερείς δομές διακυβέρνησης σε διεθνές επίπεδο. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι όλοι οι τύποι πρόσβασης σε προσωπικά και μη προσωπικά δεδομένα καταχώρισης ονομάτων τομέα είναι δωρεάν.

(113) Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένες. Ωστόσο, οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. Οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD, οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, οι πάροχοι υπηρεσιών υπολογιστικού νέφους, οι πάροχοι υπηρεσιών κέντρων δεδομένων, οι πάροχοι δικτύων διανομής περιεχομένου, οι πάροχοι διαχειριζομένων υπηρεσιών, οι πάροχοι διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και οι πάροχοι επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης θα πρέπει να θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση. Οι οντότητες της δημόσιας διοίκησης πρέπει να υπάγονται στη δικαιοδοσία του κράτους μέλους που τις έχει συστήσει. Εάν η οντότητα παρέχει υπηρεσίες ή είναι εγκατεστημένη σε περισσότερα του ενός κράτη μέλη, θα πρέπει να υπάγεται στη χωριστή και συντρέχουσα δικαιοδοσία καθενός από αυτά τα κράτη μέλη. Οι αρμόδιες αρχές των εν λόγω κρατών μελών θα πρέπει να συνεργάζονται, να παρέχουν αμοιβαία συνδρομή μεταξύ τους και, κατά περίπτωση, να εκτελούν κοινές εποπτικές δράσεις. Όταν τα κράτη μέλη ασκούν δικαιοδοσία, δεν θα πρέπει να προβλέπουν πάνω από μία φορά μέτρα επιβολής ή κυρώσεις για την ίδια συμπεριφορά, σύμφωνα με την αρχή ne bis in idem.

(114) Προκειμένου να ληφθεί υπόψη ο διασυνοριακός χαρακτήρας των υπηρεσιών και των λειτουργιών των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, των παρόχων υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων διαχειριζομένων υπηρεσιών, των παρόχων διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και των παρόχων επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, μόνο ένα κράτος μέλος θα πρέπει να έχει δικαιοδοσία επί των εν λόγω οντοτήτων. Η δικαιοδοσία θα πρέπει να ανατίθεται στο κράτος μέλος στο οποίο η οικεία οντότητα έχει την κύρια εγκατάστασή της στην Ένωση. Το κριτήριο της εγκατάστασης για τους σκοπούς της παρούσας οδηγίας συνεπάγεται την πραγματική άσκηση δραστηριότητας μέσω σταθερών ρυθμίσεων. Από αυτή την άποψη, ο νομικός τύπος των ρυθμίσεων αυτών, είτε πρόκειται για παράρτημα είτε για θυγατρική με νομική προσωπικότητα, δεν είναι καθοριστικής σημασίας. Το κατά πόσον πληρούται το συγκεκριμένο κριτήριο δεν θα πρέπει να εξαρτάται από το αν τα συστήματα δικτύου και πληροφοριών βρίσκονται σε συγκεκριμένο τόπο· η παρουσία και η χρήση τέτοιων συστημάτων δεν συνιστούν από μόνες τους βασική εγκατάσταση και συνεπώς δεν συνιστούν αποφασιστικά κριτήρια για τον καθορισμό της βασικής εγκατάστασης. Η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι είναι στο κράτος μέλος όπου λαμβάνονται κατά κύριο λόγο στην Ένωση οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. Αυτό συνήθως αντιστοιχεί στον τόπο της κεντρικής διοίκησης των οντοτήτων εντός της Ένωσης. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί ή εάν δεν ληφθούν τέτοιες αποφάσεις στην Ένωση, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο διεξάγονται οι επιχειρήσεις κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο η οντότητα έχει την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση. Όταν οι υπηρεσίες παρέχονται από όμιλο επιχειρήσεων, η κύρια εγκατάσταση της ελέγχουσας επιχείρησης θα πρέπει να θεωρείται ως η κύρια εγκατάσταση του ομίλου επιχειρήσεων.

(115) Όταν μια διαθέσιμη στο κοινό υπηρεσία DNS παρέχεται από πάροχο δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών μόνο ως μέρος της υπηρεσίας πρόσβασης στο διαδίκτυο, η οντότητα θα πρέπει να θεωρείται ότι εμπίπτει στη δικαιοδοσία όλων των κρατών μελών στα οποία παρέχονται οι υπηρεσίες της.

(116) Όταν πάροχος υπηρεσιών DNS, μητρώο ονομάτων TLD, οντότητα που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα, πάροχος υπηρεσιών υπολογιστικού νέφους, πάροχος υπηρεσιών κέντρου δεδομένων, πάροχος δικτύου διανομής περιεχομένου, πάροχος διαχειριζομένων υπηρεσιών, πάροχος διαχειριζομένων υπηρεσιών ασφάλειας ή πάροχος επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών κοινωνικής δικτύωσης, ο οποίος δεν είναι εγκατεστημένος στην Ένωση, προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να ορίζει εκπρόσωπο στην Ένωση. Για να προσδιοριστεί κατά πόσον μια τέτοια οντότητα προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να εξακριβώνεται αν η εν λόγω οντότητα σχεδιάζει να προσφέρει υπηρεσίες σε πρόσωπα σε ένα η περισσότερα κράτη μέλη. Η απλή προσβασιμότητα στην Ένωση του δικτυακού τόπου της οντότητας ή ενός ενδιάμεσου φορέα ή μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου ή άλλων στοιχείων επικοινωνίας, ή η χρήση γλώσσας που χρησιμοποιείται γενικά στην τρίτη χώρα όπου είναι εγκατεστημένη η οντότητα θα πρέπει να θεωρείται ανεπαρκής για την επιβεβαίωση της εν λόγω πρόθεσης. Ωστόσο, παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιείται γενικά σε ένα ή περισσότερα κράτη μέλη με δυνατότητα παραγγελίας υπηρεσιών στη γλώσσα αυτή, ή η αναφορά πελατών ή χρηστών που βρίσκονται στην Ένωση, θα μπορούσαν να καταστήσουν σαφές ότι η οντότητα σχεδιάζει να προσφέρει υπηρεσίες εντός της Ένωσης. Ο εκπρόσωπος πρέπει να ενεργεί εξ ονόματος της οντότητας και οι αρμόδιες αρχές ή οι CSIRT θα πρέπει να έχουν τη δυνατότητα να απευθύνονται στον εκπρόσωπο. Ο εκπρόσωπος θα πρέπει να ορίζεται ρητώς με γραπτή εντολή της οντότητας να ενεργεί για λογαριασμό της τελευταίας όσον αφορά τις υποχρεώσεις της που απορρέουν από την παρούσα οδηγία, συμπεριλαμβανομένης της αναφοράς περιστατικών.

(117) Προκειμένου να διασφαλιστεί σαφής επισκόπηση των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, των οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, των παρόχων υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των παρόχων δικτύων διανομής περιεχομένου, των παρόχων διαχειριζομένων υπηρεσιών, των παρόχων διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και των παρόχων επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης, οι οποίες παρέχουν υπηρεσίες σε ολόκληρη την Ένωση που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, ο ENISA θα πρέπει να δημιουργήσει και να τηρεί μητρώο των εν λόγω οντοτήτων, με βάση τις πληροφορίες που λαμβάνουν τα κράτη μέλη, κατά περίπτωση μέσω εθνικών μηχανισμών που έχουν θεσπιστεί για την καταχώριση των οντοτήτων. Τα ενιαία σημεία επαφής θα πρέπει να διαβιβάζουν στον ENISA τις πληροφορίες και τυχόν αλλαγές τους. Προκειμένου να εξασφαλίζονται η ακρίβεια και η πληρότητα των πληροφοριών που πρέπει να περιλαμβάνονται στο εν λόγω μητρώο, τα κράτη μέλη μπορούν να υποβάλλουν στον ENISA τις πληροφορίες που είναι διαθέσιμες σε τυχόν εθνικά μητρώα των εν λόγω οντοτήτων. Ο ENISA και τα κράτη μέλη θα πρέπει να λάβουν μέτρα για να διευκολύνουν τη διαλειτουργικότητα των εν λόγω μητρώων, διασφαλίζοντας παράλληλα την προστασία των εμπιστευτικών ή διαβαθμισμένων πληροφοριών. Ο ENISA θα πρέπει να θεσπίζει κατάλληλα πρωτόκολλα ταξινόμησης και διαχείρισης πληροφοριών για την εγγύηση της ασφάλειας και της εμπιστευτικότητας γνωστοποιημένων πληροφοριών, και να περιορίζει την πρόσβαση, αποθήκευση και διαβίβαση τέτοιου είδους πληροφοριών στους χρήστες για τους οποίους προορίζονται.

(118) Όταν οι πληροφορίες που είναι διαβαθμισμένες σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, ανταλλάσσονται, αναφέρονται ή κοινοποιούνται με άλλον τρόπο δυνάμει της παρούσας οδηγίας, θα πρέπει να εφαρμόζονται οι αντίστοιχοι κανόνες για τον χειρισμό των διαβαθμισμένων πληροφοριών. Επιπλέον, ο ENISA θα πρέπει να διαθέτει υποδομές, διαδικασίες και κανόνες ώστε να χειρίζεται ευαίσθητες και διαβαθμισμένες πληροφορίες σύμφωνα με τους ισχύοντες κανόνες ασφάλειας της ΕΕ για την προστασία διαβαθμισμένων πληροφοριών.

(119) Καθώς οι κυβερνοαπειλές καθίστανται πιο σύνθετες και εξελιγμένες, ο ορθός εντοπισμός αυτών των απειλών και τα μέτρα για την πρόληψή τους εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών σχετικά με απειλές και τρωτότητες μεταξύ των οντοτήτων. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, γεγονός που, με τη σειρά του, ενισχύει την ικανότητα των οντοτήτων να αποτρέπουν την επέλευση τέτοιων απειλών σε περιστατικά και επιτρέπει στις οντότητες να περιορίζουν καλύτερα τις επιπτώσεις των περιστατικών και να ανακάμπτουν αποτελεσματικότερα. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης, διάφοροι παράγοντες φαίνεται ότι εμπόδισαν την εν λόγω ανταλλαγή πληροφοριών, ιδίως η αβεβαιότητα σχετικά με τη συμβατότητα με τους κανόνες περί ανταγωνισμού και ευθύνης.

(120) Οι οντότητες θα πρέπει να ενθαρρύνονται και να επικουρούνται από τα κράτη μέλη ώστε να αξιοποιούν συλλογικά τις ατομικές γνώσεις και την πρακτική πείρα τους σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους να προλαμβάνουν, να εντοπίζουν, να αντιμετωπίζουν ή να ανακάμπτουν από περιστατικά ή να μετριάζουν τις επιπτώσεις τους. Συνεπώς, είναι αναγκαίο να καταστεί δυνατή η δημιουργία ρυθμίσεων εθελοντικής ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να συνδράμουν ενεργά και να ενθαρρύνουν επίσης οντότητες όπως αυτές που παρέχουν υπηρεσίες και έρευνα κυβερνοασφάλειας, καθώς και τις σχετικές οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, να συμμετέχουν στις εν λόγω ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας. Οι ρυθμίσεις αυτές θα πρέπει να θεσπιστούν σε πλήρη συμμόρφωση με τους κανόνες ανταγωνισμού της Ένωσης και το δίκαιο της Ένωσης για την προστασία των δεδομένων.

(121) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αναγκαία και αναλογική για τον σκοπό της προστασίας της ασφάλειας των συστημάτων δικτύου και πληροφοριών από βασικές και σημαντικές οντότητες, θα μπορούσε να θεωρηθεί σύννομη λόγω του ότι η εν λόγω επεξεργασία συμμορφώνεται με νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, σύμφωνα με τις απαιτήσεις του άρθρου 6 παράγραφος 1 στοιχείο γ) και του άρθρου 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε επίσης να είναι απαραίτητη για έννομα συμφέροντα που επιδιώκονται από βασικές και σημαντικές οντότητες, καθώς και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας που ενεργούν για λογαριασμό των εν λόγω οντοτήτων, σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ) του κανονισμού (ΕΕ) 2016/679, μεταξύ άλλων όταν η εν λόγω επεξεργασία είναι απαραίτητη για ρυθμίσεις ανταλλαγής πληροφοριών για την κυβερνοασφάλεια ή για την εθελοντική κοινοποίηση σχετικών πληροφοριών σύμφωνα με την παρούσα οδηγία. Μέτρα σχετικά με την πρόληψη, τον εντοπισμό, τον προσδιορισμό, τον περιορισμό, την ανάλυση και την αντιμετώπιση περιστατικών, μέτρα για την ευαισθητοποίηση σχετικά με συγκεκριμένες κυβερνοαπειλές, την ανταλλαγή πληροφοριών στο πλαίσιο της αποκατάστασης ευπαθειών και της συντονισμένης γνωστοποίησης ευπαθειών, την εθελούσια ανταλλαγή πληροφοριών σχετικά με τα εν λόγω περιστατικά, τις κυβερνοαπειλές και τις ευπάθειες, τους δείκτες έκθεσης σε κίνδυνο, τις τακτικές, τις τεχνικές και τις διαδικασίες, τις ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και τα εργαλεία διαμόρφωσης θα μπορούσαν να απαιτούν την επεξεργασία ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως διευθύνσεις IP, ενιαίους εντοπιστές πόρων (URL), ονόματα τομέα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, και, στον βαθμό που αυτά αποκαλύπτουν προσωπικά δεδομένα, χρονοσφραγίδες. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές, ενιαία σημεία επαφής και CSIRT θα μπορούσε να συνιστά νομική υποχρέωση ή να θεωρείται αναγκαία για την εκτέλεση καθήκοντος δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο γ) ή ε) και το άρθρο 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679, ή για την επιδίωξη έννομου συμφέροντος των βασικών και σημαντικών οντοτήτων, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού. Επιπλέον, το εθνικό δίκαιο θα μπορούσε να θεσπίζει κανόνες που θα επιτρέπουν στις αρμόδιες αρχές, στα ενιαία σημεία επαφής και στις CSIRT, στον βαθμό που είναι αναγκαίο και αναλογικό για τον σκοπό της προστασίας της ασφάλειας των συστημάτων δικτύου και πληροφοριών βασικών και σημαντικών οντοτήτων, να επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) 2016/679, ιδίως με την πρόβλεψη κατάλληλων και ειδικών μέτρων για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων των φυσικών προσώπων, συμπεριλαμβανομένων τεχνικών περιορισμών στην περαιτέρω χρήση των εν λόγω δεδομένων και της χρήσης προηγμένων μέτρων ασφάλειας και προστασίας της ιδιωτικής ζωής, όπως η ψευδωνυμοποίηση, ή η κρυπτογράφηση όταν η ανωνυμοποίηση μπορεί να επηρεάσει σημαντικά τον επιδιωκόμενο σκοπό.

(122) Προκειμένου να ενισχυθούν οι εποπτικές εξουσίες και τα μέτρα που συμβάλλουν στη διασφάλιση της αποτελεσματικής συμμόρφωσης, η παρούσα οδηγία θα πρέπει να προβλέπει έναν ελάχιστο κατάλογο εποπτικών μέτρων και μέσων μέσω των οποίων οι αρμόδιες αρχές μπορούν να εποπτεύουν βασικές και σημαντικές οντότητες. Επιπλέον, η παρούσα οδηγία θα πρέπει να καθιερώσει μια διαφοροποίηση του εποπτικού καθεστώτος μεταξύ βασικών και σημαντικών οντοτήτων, με σκοπό την εξασφάλιση δίκαιης ισορροπίας των υποχρεώσεων τόσο για τις εν λόγω οντότητες όσο και για τις αρμόδιες αρχές. Συνεπώς, οι βασικές οντότητες θα πρέπει να υπόκεινται σε πλήρες εκ των προτέρων και εκ των υστέρων καθεστώς εποπτείας, ενώ οι σημαντικές οντότητες θα πρέπει να υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς. Δεν θα πρέπει επομένως να απαιτείται από τις σημαντικές οντότητες να τεκμηριώνουν συστηματικά τη συμμόρφωση με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, ενώ οι αρμόδιες αρχές θα πρέπει να εφαρμόζουν μια εκ των υστέρων προσέγγιση της εποπτείας και, ως εκ τούτου, να μην έχουν γενική υποχρέωση εποπτείας των εν λόγω οντοτήτων. Η εκ των υστέρων εποπτεία σημαντικών οντοτήτων μπορεί να ενεργοποιείται με αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες που περιέρχονται σε γνώση των αρμόδιων αρχών τις οποίες οι εν λόγω αρχές θεωρούν ότι υποδηλώνουν πιθανές παραβιάσεις των υποχρεώσεων της παρούσας οδηγίας. Για παράδειγμα, τέτοια αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες θα μπορούσαν να είναι του είδους που παρέχονται στις αρμόδιες αρχές από άλλες αρχές, οντότητες, πολίτες, μέσα ενημέρωσης ή άλλες πηγές, πληροφορίες διαθέσιμες στο κοινό, ή θα μπορούσαν να προκύπτουν από άλλες δραστηριότητες που διεξάγουν οι αρμόδιες αρχές κατά την εκτέλεση των καθηκόντων τους.

(123) Η εκτέλεση εποπτικών καθηκόντων από τις αρμόδιες αρχές δεν θα πρέπει να παρεμποδίζει αδικαιολόγητα τις επιχειρηματικές δραστηριότητες της οικείας οντότητας. Όταν οι αρμόδιες αρχές εκτελούν τα εποπτικά τους καθήκοντα σε σχέση με βασικές οντότητες, συμπεριλαμβανομένης της διενέργειας επιτόπιων επιθεωρήσεων και της εποπτείας εκτός των εγκαταστάσεων, της διερεύνησης περιπτώσεων παραβιάσεων της παρούσας οδηγίας, και της διενέργειας ελέγχων ασφάλειας ή σαρώσεων ασφαλείας, θα πρέπει να ελαχιστοποιούν τον αντίκτυπο στις επιχειρηματικές δραστηριότητες της οικείας οντότητας.

(124) Στο πλαίσιο της άσκησης της εκ των προτέρων εποπτείας, οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να αποφασίζουν πώς θα ιεραρχήσουν τη χρήση των εποπτικών μέτρων και μέσων που έχουν στη διάθεσή τους με αναλογικό τρόπο. Τούτο συνεπάγεται ότι οι αρμόδιες αρχές μπορούν να αποφασίζουν σχετικά με την εν λόγω ιεράρχηση βάσει εποπτικών μεθοδολογιών οι οποίες θα πρέπει να ακολουθούν προσέγγιση που βασίζεται στους κινδύνους. Πιο συγκεκριμένα, οι μεθοδολογίες αυτές θα μπορούσαν να περιλαμβάνουν κριτήρια ή στοιχεία αναφοράς για την κατάταξη των βασικών οντοτήτων σε κατηγορίες κινδύνου, και αντίστοιχα εποπτικά μέτρα και μέσα που συνιστώνται ανά κατηγορία κινδύνου, όπως χρήση, συχνότητα ή είδος επιτόπιων επιθεωρήσεων, ή στοχευμένων ελέγχων ασφαλείας ή σαρώσεων ασφαλείας, είδος πληροφοριών που πρέπει να ζητούνται και βαθμός λεπτομέρειας των εν λόγω πληροφοριών. Οι εν λόγω εποπτικές

μεθοδολογίες θα μπορούσαν επίσης να συνοδεύονται από προγράμματα εργασίας και να αξιολογούνται και να επανεξετάζονται τακτικά, μεταξύ άλλων όσον αφορά πτυχές όπως η κατανομή των πόρων και οι ανάγκες σε πόρους. Όσον αφορά τους φορείς δημόσιας διοίκησης, οι εποπτικές εξουσίες θα πρέπει να ασκούνται σύμφωνα με το εθνικό νομοθετικό και θεσμικό πλαίσιο.

(125) Οι αρμόδιες αρχές θα πρέπει να διασφαλίζουν ότι τα εποπτικά τους καθήκοντα σε σχέση με βασικές και σημαντικές οντότητες ασκούνται από καταρτισμένους επαγγελματίες, οι οποίοι θα πρέπει να διαθέτουν τις απαραίτητες δεξιότητες για την εκτέλεση των εν λόγω καθηκόντων, ιδίως όσον αφορά τη διενέργεια επιτόπιων επιθεωρήσεων και την εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένου του εντοπισμού αδυναμιών στις βάσεις δεδομένων, το υλικό, τα τείχη προστασίας, την κρυπτογράφηση και τα δίκτυα. Οι εν λόγω επιθεωρήσεις και εποπτεία θα πρέπει να διενεργούνται με αντικειμενικό τρόπο.

(126) Σε δεόντως αιτιολογημένες περιπτώσεις όπου αντιλαμβάνεται σημαντική κυβερνοαπειλή ή επικείμενο κίνδυνο, η αρμόδια αρχή θα πρέπει να είναι σε θέση να λαμβάνει άμεσες αποφάσεις επιβολής με σκοπό την πρόληψη ή την αντιμετώπιση περιστατικού.

(127) Προκειμένου να καταστεί αποτελεσματική η επιβολή, θα πρέπει να καταρτιστεί ένας ελάχιστος κατάλογος μέσων επιβολής που μπορούν να ασκηθούν σε περίπτωση παραβίασης των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων που προβλέπονται στην παρούσα οδηγία, με τη θέσπιση σαφούς και συνεκτικού πλαισίου για τα εν λόγω μέσα επιβολής σε ολόκληρη την Ένωση. Θα πρέπει να λαμβάνονται δεόντως υπόψη η φύση, η σοβαρότητα και η διάρκεια της παράβασης της παρούσας οδηγίας, η υλική ή μη υλική ζημία που προκλήθηκε, το κατά πόσον η παράβαση ήταν εκ προθέσεως ή εξ αμελείας, οι ενέργειες που πραγματοποιήθηκαν για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας, ο βαθμός ευθύνης ή τυχόν σχετικών προηγούμενων παραβάσεων, ο βαθμός συνεργασίας με την αρμόδια αρχή και κάθε άλλη επιβαρυντική ή ελαφρυντική περίσταση. Τα μέσα επιβολής, περιλαμβανομένων των διοικητικών προστίμων, θα πρέπει να είναι αναλογικές και η επιβολή τους θα πρέπει να υπόκειται σε κατάλληλες δικονομικές εγγυήσεις σύμφωνα με τις γενικές αρχές του ενωσιακού δικαίου και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («ο Χάρτης»), συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και του δικαιώματος υπεράσπισης.

(128) Η παρούσα οδηγία δεν απαιτεί από τα κράτη μέλη να προβλέπουν ποινική ή αστική ευθύνη έναντι φυσικών προσώπων που είναι υπεύθυνα να διασφαλίζουν ότι μια οντότητα συμμορφώνεται με την παρούσα οδηγία για ζημία που υπέστησαν τρίτοι ως αποτέλεσμα παραβίασης της παρούσας οδηγίας.

(129) Προκειμένου να διασφαλιστεί η αποτελεσματική επιβολή των υποχρεώσεων που ορίζονται στην παρούσα οδηγία, κάθε αρμόδια αρχή θα πρέπει να έχει την εξουσία να επιβάλλει ή να ζητεί την επιβολή διοικητικών προστίμων.

(130) Σε περίπτωση που επιβάλλονται διοικητικά πρόστιμα σε βασική ή σημαντική οντότητα που είναι επιχείρηση, η επιχείρηση θα πρέπει να νοείται ως επιχείρηση σύμφωνα με τα άρθρα 101 και 102 ΣΛΕΕ για τους σκοπούς αυτούς. Σε περίπτωση που επιβάλλονται διοικητικά πρόστιμα σε πρόσωπα που δεν είναι επιχειρήσεις, η αρμόδια αρχή θα πρέπει να λαμβάνει υπόψη το γενικό επίπεδο εισοδημάτων στο κράτος μέλος, καθώς και την οικονομική κατάσταση του προσώπου, όταν εξετάζει το ενδεδειγμένο ποσό του προστίμου. Θα πρέπει να εναπόκειται στα κράτη μέλη να αποφασίζουν εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε δημόσιες αρχές. Η επιβολή διοικητικού προστίμου δεν θίγει την άσκηση άλλων εξουσιών από τις αρμόδιες αρχές ή άλλων κυρώσεων που προβλέπονται στους εθνικούς κανόνες μεταφοράς της παρούσας οδηγίας.

(131) Τα κράτη μέλη θα πρέπει να μπορούν να θεσπίζουν κανόνες σχετικά με τις ποινικές κυρώσεις για παραβάσεις των εθνικών κανόνων μεταφοράς της παρούσας οδηγίας. Ωστόσο, η επιβολή ποινικών κυρώσεων για παραβάσεις τέτοιων εθνικών κανόνων και συναφών διοικητικών κυρώσεων δεν θα πρέπει να οδηγεί σε παραβίαση της αρχής ne bis in idem, όπως την ερμηνεύει το Δικαστήριο της Ευρωπαϊκής Ένωσης.

(132) Όταν η παρούσα οδηγία δεν εναρμονίζει τις διοικητικές κυρώσεις ή όταν είναι αναγκαίο σε άλλες περιπτώσεις, π.χ. σε περίπτωση σοβαρής παράβασης των υποχρεώσεων της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να εφαρμόζουν σύστημα που προβλέπει αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις. Η φύση των εν λόγω κυρώσεων (ποινικών ή διοικητικών) θα πρέπει να προσδιορίζεται από το εθνικό δίκαιο.

(133) Προκειμένου να ενισχυθεί περαιτέρω η αποτελεσματικότητα και η αποτρεπτικότητα των εφαρμοστέων μέσων επιβολής σε περίπτωση παράβασης των υποχρεώσεων της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να έχουν την εξουσία να αναστέλλουν προσωρινά ή να ζητούν την προσωρινή αναστολή πιστοποίησης ή εξουσιοδότησης που αφορά μέρος ή το σύνολο των σχετικών υπηρεσιών που παρέχονται ή των δραστηριοτήτων που ασκούνται από βασική οντότητα και να ζητούν την επιβολή προσωρινής απαγόρευσης της άσκησης διευθυντικών καθηκόντων από οποιοδήποτε φυσικό πρόσωπο ασκεί διευθυντικά καθήκοντα σε επίπεδο διευθύνοντος συμβούλου ή νομικού εκπροσώπου. Δεδομένης της σοβαρότητας και του αντικτύπου τους στις δραστηριότητες των οντοτήτων και, εν τέλει, στους χρήστες, οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις θα πρέπει να εφαρμόζονται μόνο κατ' αναλογία προς τη σοβαρότητα της παράβασης και λαμβανομένων υπόψη των περιστάσεων κάθε μεμονωμένης περίπτωσης, συμπεριλαμβανομένου του κατά πόσον η παράβαση ήταν εκ προθέσεως ή εξ αμελείας, καθώς και οποιωνδήποτε ενεργειών που αναλαμβάνονται για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας. Οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις θα πρέπει να εφαρμόζονται μόνο ως έσχατη λύση, δηλαδή μόνο αφού εξαντληθούν τα άλλα σχετικά μέτρα επιβολής που προβλέπονται στην παρούσα οδηγία, και μόνο έως ότου η οικεία οντότητα λάβει τα αναγκαία μέτρα για να διορθώσει τις ελλείψεις ή να συμμορφωθεί με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες εφαρμόστηκαν οι εν λόγω προσωρινές αναστολές ή απαγορεύσεις. Η επιβολή τέτοιων προσωρινών αναστολών ή απαγορεύσεων θα πρέπει να υπόκειται σε κατάλληλες διαδικαστικές εγγυήσεις σύμφωνα με τις γενικές αρχές του δικαίου της Ένωσης και του Χάρτη, συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και του δικαιώματος υπεράσπισης.

(134) Για τη διασφάλιση της συμμόρφωσης των οντοτήτων με τις υποχρεώσεις τους δυνάμει της παρούσας οδηγίας, τα κράτη μέλη θα πρέπει να συνεργάζονται και να αλληλοβοηθούνται όσον αφορά τα μέτρα εποπτείας και επιβολής, ιδίως όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη ή όταν τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε κράτος μέλος διαφορετικό από εκείνο στο οποίο παρέχει υπηρεσίες. Κατά την παροχή συνδρομής, η αρμόδια αρχή στην οποία υποβάλλεται το αίτημα θα πρέπει να λαμβάνει μέτρα εποπτείας ή επιβολής σύμφωνα με το εθνικό δίκαιο. Προκειμένου να διασφαλιστεί η ομαλή λειτουργία της αμοιβαίας συνδρομής δυνάμει της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να χρησιμοποιούν την Ομάδα Συνεργασίας ως φόρουμ για τη συζήτηση υποθέσεων και ειδικών αιτημάτων συνδρομής.

(135) Προκειμένου να διασφαλιστεί η αποτελεσματική εποπτεία και επιβολή, ιδίως σε περίπτωση κατάστασης με διασυνοριακή διάσταση, τα κράτη μέλη που έχουν λάβει αίτηση αμοιβαίας συνδρομής θα πρέπει, εντός των ορίων του εν λόγω αιτήματος, να λαμβάνουν κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οντότητα αποτελεί αντικείμενο του αιτήματος αυτού και που παρέχει υπηρεσίες ή διαθέτει σύστημα δικτύου και πληροφοριών στην επικράτειά τους.

(136) Η παρούσα οδηγία θα πρέπει να θεσπίσει κανόνες συνεργασίας μεταξύ των αρμόδιων αρχών και των εποπτικών αρχών δυνάμει του κανονισμού (ΕΕ) 2016/679 για την αντιμετώπιση παραβάσεων της παρούσας οδηγίας που σχετίζονται με δεδομένα προσωπικού χαρακτήρα.

(137) Η παρούσα οδηγία θα πρέπει να αποσκοπεί στη διασφάλιση υψηλού επιπέδου ευθύνης για τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις υποβολής εκθέσεων στο επίπεδο των βασικών και σημαντικών οντοτήτων. Συνεπώς, τα διοικητικά όργανα των βασικών και σημαντικών οντοτήτων θα πρέπει να εγκρίνουν τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και να επιβλέπουν την εφαρμογή τους.

(138) Προκειμένου να διασφαλιστεί υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση βάσει της παρούσας οδηγίας, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 ΣΛΕΕ όσον αφορά τη συμπλήρωση της παρούσας οδηγίας με τον προσδιορισμό των κατηγοριών βασικών και σημαντικών οντοτήτων που πρέπει να χρησιμοποιούν ορισμένα πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ ή να αποκτούν πιστοποιητικό στο πλαίσιο ευρωπαϊκού καθεστώτος πιστοποίησης κυβερνοασφάλειας. Είναι ιδιαίτερα σημαντικό η Επιτροπή να διεξάγει, κατά τις προπαρασκευαστικές της εργασίες, τις κατάλληλες διαβουλεύσεις, μεταξύ άλλων σε επίπεδο εμπειρογνωμόνων, και οι διαβουλεύσεις αυτές να πραγματοποιούνται σύμφωνα με τις αρχές που ορίζονται στη διοργανική συμφωνία της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου ([22]). Πιο συγκεκριμένα, προκειμένου να διασφαλιστεί η ίση συμμετοχή στην προετοιμασία των κατ' εξουσιοδότηση πράξεων, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο λαμβάνουν όλα τα έγγραφα κατά τον ίδιο χρόνο με τους εμπειρογνώμονες των κρατών μελών, και οι εμπειρογνώμονές τους έχουν συστηματικά πρόσβαση στις συνεδριάσεις των ομάδων εμπειρογνωμόνων της Επιτροπής που ασχολούνται με την προετοιμασία κατ' εξουσιοδότηση πράξεων.

([22]) ΕΕ L 123 της 12.5.2016, σ. 1.

(139) Προκειμένου να διασφαλιστούν ενιαίες προϋποθέσεις για την εφαρμογή της παρούσας οδηγίας, θα πρέπει να ανατεθούν στην Επιτροπή εκτελεστικές αρμοδιότητες για τον καθορισμό των διαδικαστικών ρυθμίσεων που απαιτούνται για τη λειτουργία της ομάδας συνεργασίας και των τεχνικών και μεθοδολογικών και τομεακών απαιτήσεων σχετικά με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, καθώς και για τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφότυπου και της διαδικασίας των κοινοποιήσεων περιστατικών, κυβερνοαπειλών και κοινοποιήσεων παρ' ολίγον περιστατικών, και της κοινοποίησης σημαντικών κυβερνοαπειλών, καθώς και των περιπτώσεων στις οποίες ένα περιστατικό πρέπει να θεωρείται σημαντικό. Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([23]).

(140) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά την παρούσα οδηγία, κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, ιδίως προκειμένου να καθορίζεται κατά πόσον είναι σκόπιμο να προτείνονται τροποποιήσεις υπό το φως αλλαγών στις κοινωνικές, πολιτικές, τεχνολογικές συνθήκες ή στις συνθήκες της αγοράς. Στο πλαίσιο των εν λόγω επανεξετάσεων, η Επιτροπή θα πρέπει να αξιολογεί τη συνάφεια του μεγέθους των οικείων οντοτήτων και των τομέων, των υποτομέων και των τύπων οντοτήτων που αναφέρονται στα παραρτήματα της παρούσας οδηγίας για τη λειτουργία της οικονομίας και της κοινωνίας σε σχέση με την κυβερνοασφάλεια. Η Επιτροπή θα πρέπει να αξιολογεί, μεταξύ άλλων, κατά πόσον οι πάροχοι που χαρακτηρίζονται ως πολύ μεγάλες επιγραμμικές πλατφόρμες κατά την έννοια του άρθρου 33 του κανονισμού (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([24]) θα μπορούσαν να χαρακτηριστούν βασικές οντότητες βάσει της παρούσας οδηγίας.

(141) Η παρούσα οδηγία δημιουργεί νέα καθήκοντα για τον ENISA, ενισχύοντας έτσι τον ρόλο του, και θα μπορούσε επίσης να έχει ως αποτέλεσμα να απαιτείται από τον ENISA να εκτελεί τα υφιστάμενα καθήκοντά του δυνάμει του κανονισμού (ΕΕ) 2019/881 σε υψηλότερο επίπεδο από ό, τι στο παρελθόν. Προκειμένου να διασφαλιστεί ότι ο ENISA διαθέτει τους αναγκαίους οικονομικούς και ανθρώπινους πόρους για την εκτέλεση των υφιστάμενων και των νέων καθηκόντων, καθώς και για την κάλυψη οποιουδήποτε υψηλότερου επιπέδου εκτέλεσης των εν λόγω καθηκόντων που απορρέει από τον ενισχυμένο ρόλο του, ο προϋπολογισμός του θα πρέπει να αυξηθεί αναλόγως. Επιπλέον, προκειμένου να διασφαλιστεί η αποδοτική χρήση των πόρων, ο ENISA θα πρέπει να διαθέτει μεγαλύτερη ευελιξία όσον αφορά τον τρόπο με τον οποίο είναι σε θέση να κατανέμει τους πόρους εσωτερικά με σκοπό την αποτελεσματική εκτέλεση των καθηκόντων του και την ικανοποίηση των προσδοκιών.

(142) Δεδομένου ότι ο στόχος της παρούσας οδηγίας, ήτοι η επίτευξη υψηλού ενιαίου επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, δεν μπορεί να επιτευχθεί ικανοποιητικά από τα κράτη μέλη αλλά μπορεί, λόγω των επιπτώσεων της δράσης, να επιτευχθεί καλύτερα σε ενωσιακό επίπεδο, η Ένωση μπορεί να λάβει μέτρα, σύμφωνα με την αρχή της επικουρικότητας του άρθρου 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας του ιδίου άρθρου, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία για την επίτευξη του στόχου αυτού.

(143) Η παρούσα οδηγία σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη, ιδίως το δικαίωμα στον σεβασμό της ιδιωτικότητας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την επιχειρηματική ελευθερία, το δικαίωμα ιδιοκτησίας, το δικαίωμα αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, το τεκμήριο αθωότητας και το δικαίωμα υπεράσπισης. Το δικαίωμα αποτελεσματικής δικαστικής προστασίας εκτείνεται στους αποδέκτες υπηρεσιών που παρέχονται από βασικές και σημαντικές οντότητες. Η παρούσα οδηγία θα πρέπει να εφαρμόζεται σύμφωνα με τα δικαιώματα και τις αρχές αυτές.

(144) Ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([25]) και διατύπωσε γνώμη στις 11 Μαρτίου 2021 ([26]),

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

([24]) Κανονισμός (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Οκτωβρίου 2022, σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της οδηγίας 2000/31/ΕΚ (πράξη για τις ψηφιακές υπηρεσίες) (ΕΕ L 277 της 27.10.2022, σ. 1).

([25]) 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).

([26]) ΕΕ C 183 της 11.5.2021, σ. 3.

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

1. Η παρούσα οδηγία θεσπίζει μέτρα που αποσκοπούν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, με σκοπό τη βελτίωση της λειτουργίας της εσωτερικής αγοράς.

2. Για τον σκοπό αυτό, η παρούσα οδηγία καθορίζει:

α) υποχρεώσεις που απαιτούν από τα κράτη μέλη να εγκρίνουν εθνικές στρατηγικές κυβερνοασφάλειας και να ορίσουν ή να συστήσουν αρμόδιες αρχές, αρχές διαχείρισης κυβερνοκρίσεων, ενιαία σημεία επαφής για την κυβερνοασφάλεια (ενιαία σημεία επαφής) και ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)·

β) μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις υποβολής αναφορών για οντότητες του τύπου που αναφέρεται στο παράρτημα I ή II καθώς και για οντότητες που χαρακτηρίζονται ως κρίσιμες δυνάμει της οδηγίας (ΕΕ) 2022/2557·

γ) κανόνες και υποχρεώσεις σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια·

δ) υποχρεώσεις των κρατών μελών σχετικά με την εποπτεία και την επιβολή.

Άρθρο 2

Πεδίο εφαρμογής

1. Η παρούσα οδηγία εφαρμόζεται σε δημόσιες ή ιδιωτικές οντότητες των τύπων που αναφέρονται στο παράρτημα I ή II οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στο εν λόγω άρθρο και οι οποίες παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ένωσης.

Το άρθρο 3 παράγραφος 4 του παραρτήματος της εν λόγω σύστασης δεν εφαρμόζεται για τους σκοπούς της παρούσας οδηγίας.

2. Ανεξάρτητα από το μέγεθός τους, η παρούσα οδηγία εφαρμόζεται επίσης στις οντότητες τύπου που αναφέρεται στο παράρτημα I ή II, εφόσον:

α) οι υπηρεσίες παρέχονται από:

i) παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών·

ii) παρόχους υπηρεσιών εμπιστοσύνης·

iii) μητρώα ονομάτων τομέα ανωτάτου επιπέδου, και παρόχους υπηρεσιών συστήματος ονομάτων τομέα·

β) η οντότητα είναι ο μοναδικός πάροχος, σε ένα κράτος μέλος, υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων κοινωνικών ή οικονομικών δραστηριοτήτων·

γ) η διατάραξη της υπηρεσίας που παρέχει η οντότητα θα μπορούσε να έχει σημαντικό αντίκτυπο στη δημόσια ασφάλεια, στη δημόσια τάξη ή στη δημόσια υγεία·

δ) η διατάραξη της υπηρεσίας που παρέχεται από την οντότητα θα μπορούσε να προκαλέσει σημαντικό συστημικό κίνδυνο, ιδίως για τομείς στους οποίους η διατάραξη αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·

ε) η οντότητα είναι κρίσιμη λόγω της ιδιαίτερης σημασίας της σε εθνικό ή περιφερειακό επίπεδο για τον συγκεκριμένο τομέα ή είδος υπηρεσίας ή για άλλους αλληλοεξαρτώμενους τομείς στο κράτος μέλος·

στ) η οντότητα είναι φορέας δημόσιας διοίκησης:

i) της κεντρικής κυβέρνησης όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο·

ii) σε περιφερειακό επίπεδο, όπως ορίζεται από κράτος μέλος σύμφωνα με το εθνικό δίκαιο, ο οποίος, μετά από αξιολόγηση βάσει κινδύνου, παρέχει υπηρεσίες των οποίων η διατάραξη θα μπορούσε να έχει σημαντικό αντίκτυπο σε κρίσιμες κοινωνικές ή οικονομικές δραστηριότητες.

3. Ανεξαρτήτως του μεγέθους τους, η παρούσα οδηγία εφαρμόζεται σε οντότητες που χαρακτηρίζονται ως κρίσιμες οντότητες δυνάμει της οδηγίας (ΕΕ) 2022/2557·

4. Ανεξαρτήτως του μεγέθους τους, η παρούσα οδηγία εφαρμόζεται σε οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα.

5. Τα κράτη μέλη μπορούν να προβλέπουν ότι η παρούσα οδηγία εφαρμόζεται:

α) σε οντότητες δημόσιας διοίκησης σε τοπικό επίπεδο·

β) σε εκπαιδευτικά ιδρύματα, ιδίως όταν διεξάγουν κρίσιμες ερευνητικές δραστηριότητες.

6. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη της ευθύνης των κρατών μελών για τη διαφύλαξη της εθνικής ασφάλειας και κυριαρχικού τους δικαιώματος να διαφυλάσσουν άλλες ουσιώδεις λειτουργίες του κράτους, συμπεριλαμβανομένων της διασφάλισης της εδαφικής ακεραιότητας του κράτους και της διατήρησης της δημόσιας τάξης.

7. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες δημόσιας διοίκησης που ασκούν τις δραστηριότητές τους στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων της πρόληψης, της διακρίβωσης, της διαπίστωσης και της δίωξης ποινικών αδικημάτων.

8. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες οντότητες που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας τάξης, της άμυνας ή της επιβολής του νόμου, συμπεριλαμβανομένων δραστηριοτήτων που σχετίζονται με την πρόληψη, τη διερεύνηση, τη διακρίβωση και τη δίωξη ποινικών αδικημάτων, ή οι οποίες παρέχουν υπηρεσίες αποκλειστικά στους φορείς δημόσιας διοίκησης που αναφέρονται στην παράγραφο 7 του παρόντος άρθρου, από τις υποχρεώσεις που ορίζονται στο άρθρο 21 ή 23 όσον αφορά τις εν λόγω δραστηριότητες ή υπηρεσίες. Στις περιπτώσεις αυτές, τα μέτρα εποπτείας και επιβολής που αναφέρονται στο κεφάλαιο VII δεν εφαρμόζονται σε σχέση με τις συγκεκριμένες δραστηριότητες ή υπηρεσίες. Όταν οι οντότητες ασκούν δραστηριότητες ή παρέχουν υπηρεσίες αποκλειστικά του τύπου που αναφέρεται στην παρούσα παράγραφο, τα κράτη μέλη μπορούν επίσης να αποφασίσουν να εξαιρέσουν τις εν λόγω οντότητες από τις υποχρεώσεις που ορίζονται στα άρθρα 3 και 27.

9. Οι παράγραφοι 7 και 8 δεν εφαρμόζονται όταν μια οντότητα ενεργεί ως πάροχος υπηρεσιών εμπιστοσύνης.

10. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες τις οποίες τα κράτη μέλη έχουν εξαιρέσει από το πεδίο εφαρμογής του κανονισμού (ΕΕ) 2022/2554 σύμφωνα με το άρθρο 2 παράγραφος 4 του εν λόγω κανονισμού.

11. Οι υποχρεώσεις που προβλέπονται στην παρούσα οδηγία δεν συνεπάγονται την παροχή πληροφοριών, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς τα ουσιώδη συμφέροντα εθνικής ασφάλειας, δημόσιας τάξης ή άμυνας των κρατών μελών.

12. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679, της οδηγίας 2002/58/ΕΚ, των οδηγιών 2011/93/ΕΕ ([27]) και 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([28]) και της οδηγίας (ΕΕ) 2022/2557.

13. Με την επιφύλαξη του άρθρου 346 ΣΛΕΕ, πληροφορίες που είναι εμπιστευτικές σύμφωνα με ενωσιακούς ή εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές σύμφωνα με την παρούσα οδηγία, μόνον εφόσον η ανταλλαγή αυτή είναι αναγκαία για την εφαρμογή της παρούσας οδηγίας. Οι ανταλλασσόμενες πληροφορίες περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς τον σκοπό της ανταλλαγής αυτής. Η ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των οικείων οντοτήτων.

([27]) Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου (ΕΕ L 335 της 17.12.2011, σ. 1).

([28]) Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).

14. Οι οντότητες, οι αρμόδιες αρχές, τα ενιαία σημεία επαφής και οι CSIRT επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στον βαθμό που είναι αναγκαίο για τους σκοπούς της παρούσας οδηγίας και σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, και πιο συγκεκριμένα η εν λόγω επεξεργασία βασίζεται στο άρθρο 6 του εν λόγω κανονισμού.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει της παρούσας οδηγίας από παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών πραγματοποιείται σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων και το δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας, ιδίως την οδηγία 2002/58/ΕΚ.

Άρθρο 3

Βασικές και σημαντικές οντότητες

1. Για τους σκοπούς της παρούσας οδηγίας, βασικές οντότητες θεωρούνται οι ακόλουθες οντότητες:

α) οντότητες των τύπων που αναφέρονται στο παράρτημα Ι, οι οποίες υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που προβλέπονται στο άρθρο 2 παράγραφος 1 του παραρτήματος της σύστασης 2003/361/ΕΚ·

β) εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανωτάτου επιπέδου, καθώς και πάροχοι υπηρεσιών DNS, ανεξάρτητα από το μέγεθός τους·

γ) πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που χαρακτηρίζονται ως μεσαίες επιχειρήσεις, δυνάμει 2 του παραρτήματος της σύστασης 2003/361/ΕΚ·

δ) οντότητες δημόσιας διοίκησης που αναφέρονται στο άρθρο 2 παράγραφος 2 στοιχείο στ) σημείο i)·

ε) οποιεσδήποτε άλλες οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ, οι οποίες προσδιορίζονται από κράτος μέλος ως βασικές οντότητες βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε)·

στ) οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557, που αναφέρονται στο άρθρο 2 παράγραφος 3 της παρούσας οδηγίας·

ζ) αν υπάρχει σχετική πρόβλεψη στο κράτος μέλος, οντότητες που το κράτος μέλος αναγνώρισε πριν από τις 16 Ιανουαρίου 2023 ως φορείς εκμετάλλευσης βασικών υπηρεσιών σύμφωνα με την οδηγία (ΕΕ) 2016/1148 ή το εθνικό δίκαιο.

2. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ, οι οποίες δεν θεωρούνται βασικές οντότητες σύμφωνα με την παράγραφο 1 του παρόντος άρθρου, θεωρούνται σημαντικές οντότητες. Σε αυτές περιλαμβάνονται οντότητες που προσδιορίζονται από τα κράτη μέλη ως σημαντικές οντότητες βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε).

3. Έως τις 17 Απριλίου 2025, τα κράτη μέλη καταρτίζουν κατάλογο βασικών και σημαντικών οντοτήτων καθώς και οντοτήτων που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα. Τα κράτη μέλη επανεξετάζουν και, κατά περίπτωση, επικαιροποιούν τον εν λόγω κατάλογο σε τακτική βάση και στη συνέχεια τουλάχιστον ανά διετία.

4. Για τους σκοπούς της κατάρτισης του καταλόγου που αναφέρεται στην παράγραφο 3, τα κράτη μέλη απαιτούν από τις οντότητες που αναφέρονται στην εν λόγω παράγραφο να υποβάλλουν τουλάχιστον τις ακόλουθες πληροφορίες στις αρμόδιες αρχές:

α) την επωνυμία της οντότητας·

β) τη διεύθυνση και τα επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των ηλεκτρονικών διευθύνσεων, των πεδίων IP και των αριθμών τηλεφώνου·

γ) κατά περίπτωση, τον σχετικό τομέα και υποτομέα που αναφέρεται στο παράρτημα Ι ή ΙΙ· και

δ) κατά περίπτωση, κατάλογο των κρατών μελών στα οποία παρέχουν υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

Οι οντότητες που αναφέρονται στην παράγραφο 3 κοινοποιούν τυχόν αλλαγές στα στοιχεία που υποβάλλονται σύμφωνα με το πρώτο εδάφιο της παρούσας παραγράφου αμελλητί και, σε κάθε περίπτωση, εντός δύο εβδομάδων από την ημερομηνία της αλλαγής.

Η Επιτροπή, με τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), θεσπίζει αμελλητί κατευθυντήριες γραμμές και υποδείγματα σχετικά με τις υποχρεώσεις που καθορίζονται στην παρούσα παράγραφο.

Τα κράτη μέλη μπορούν να θεσπίζουν εθνικούς μηχανισμούς για να εγγράφονται οι ίδιες οι οντότητες.

5. Έως τις 17 Απριλίου 2025 και στη συνέχεια ανά διετία, οι αρμόδιες αρχές κοινοποιούν:

α) στην Επιτροπή και στην Ομάδα Συνεργασίας τον αριθμό των βασικών και σημαντικών οντοτήτων που απαριθμούνται σύμφωνα με την παράγραφο 3 για κάθε τομέα και υποτομέα που αναφέρεται στο παράρτημα I ή II· και

β) στην Επιτροπή σχετικές πληροφορίες σχετικά με τον αριθμό των βασικών και σημαντικών οντοτήτων που προσδιορίζονται βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε), τον τομέα και υποτομέα που αναφέρονται στο παράρτημα I ή II στον οποίο ανήκουν, το είδος της υπηρεσίας που παρέχουν και την διάταξη βάσει των οποίων προσδιορίστηκαν, μεταξύ εκείνων που ορίζονται στο άρθρο 2 παράγραφος 2 στοιχεία β) έως ε).

6. Έως τις 17 Απριλίου 2025 και κατόπιν αιτήματος της Επιτροπής, τα κράτη μέλη μπορούν να κοινοποιούν στην Επιτροπή τα ονόματα των βασικών και σημαντικών οντοτήτων που αναφέρονται στην παράγραφο 5 στοιχείο β).

Άρθρο 4

Τομεακές νομικές πράξεις της Ένωσης

1. Όταν οι τομεακές νομικές πράξεις της Ένωσης απαιτούν από βασικές ή σημαντικές οντότητες να εγκρίνουν μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας ή να κοινοποιούν σημαντικά περιστατικά και όταν οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, οι σχετικές διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένων των διατάξεων για την εποπτεία και την επιβολή που προβλέπονται στο κεφάλαιο VII, δεν εφαρμόζονται στις εν λόγω οντότητες. Όταν οι τομεακές νομικές πράξεις της Ένωσης δεν καλύπτουν όλες τις οντότητες σε συγκεκριμένο τομέα που εμπίπτει στο πεδίο εφαρμογής της παρούσας οδηγίας, οι σχετικές διατάξεις της παρούσας οδηγίας εξακολουθούν να εφαρμόζονται στις οντότητες που δεν καλύπτονται από τις εν λόγω τομεακές νομικές πράξεις της Ένωσης.

2. Οι απαιτήσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου θεωρούνται ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία όταν:

α) τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας είναι τουλάχιστον ισοδύναμα ως προς το αποτέλεσμα με εκείνα που προβλέπονται στο άρθρο 21 παράγραφοι 1 και 2· ή

β) η τομεακή νομική πράξη της Ένωσης προβλέπει άμεση πρόσβαση, κατά περίπτωση αυτόματη και απευθείας, στις κοινοποιήσεις περιστατικών από τις CSIRT, τις αρμόδιες αρχές ή τα ενιαία σημεία επαφής δυνάμει της παρούσας οδηγίας και εάν οι απαιτήσεις για την κοινοποίηση σημαντικών περιστατικών είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με εκείνες που ορίζονται στο άρθρο 23 παράγραφοι 1 έως 6 της παρούσας οδηγίας.

3. Έως τις 17 Ιουλίου 2023, η Επιτροπή θεσπίζει κατευθυντήριες γραμμές για την αποσαφήνιση της εφαρμογής των παραγράφων 1 και 2. Η Επιτροπή επανεξετάζει τις εν λόγω κατευθυντήριες γραμμές σε τακτική βάση. Κατά την κατάρτιση των εν λόγω κατευθυντήριων γραμμών, η Επιτροπή λαμβάνει υπόψη τυχόν παρατηρήσεις της Ομάδας Συνεργασίας και του ENISA.

Άρθρο 5

Ελάχιστη εναρμόνιση

Η παρούσα οδηγία δεν εμποδίζει τα κράτη μέλη να θεσπίζουν ή να διατηρούν διατάξεις που διασφαλίζουν υψηλότερο επίπεδο κυβερνοασφάλειας, υπό την προϋπόθεση ότι οι εν λόγω διατάξεις συνάδουν με τις υποχρεώσεις των κρατών μελών δυνάμει του ενωσιακού δικαίου.

Άρθρο 6

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας, ισχύουν οι ακόλουθοι ορισμοί:

1) «δικτυακό και πληροφοριακό σύστημα»:

α) δίκτυο ηλεκτρονικών επικοινωνιών όπως ορίζεται στο άρθρο 2 σημείο 1) της οδηγίας (ΕΕ) 2018/1972·

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή συναφών συσκευών, μία ή περισσότερες από τις οποίες, σύμφωνα με ένα πρόγραμμα, διενεργούν αυτόματη επεξεργασία ψηφιακών δεδομένων· ή

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στα στοιχεία α) και β) για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους·

2) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα των συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε δεδομένο επίπεδο εμπιστοσύνης, σε κάθε συμβάν που ενδέχεται να θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή επεξεργασμένων δεδομένων ή των υπηρεσιών που προσφέρονται από τα εν λόγω συστήματα δικτύου και πληροφοριών ή είναι προσβάσιμες μέσω αυτών·

3) «κυβερνοασφάλεια»: η κυβερνοασφάλεια όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) 2019/881·

4) «εθνική στρατηγική κυβερνοασφάλειας»: συνεκτικό πλαίσιο ενός κράτους μέλους το οποίο παρέχει στρατηγικούς στόχους και προτεραιότητες στον τομέα της κυβερνοασφάλειας και της διακυβέρνησης για την επίτευξή τους στο εν λόγω κράτος μέλος·

5) «παρ' ολίγον περιστατικό»: περιστατικό το οποίο θα μπορούσε να έχει θέσει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών, αλλά το οποίο εμποδίστηκε ή δεν υλοποιήθηκε επιτυχώς·

6) «περιστατικό»: κάθε συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών·

7) «περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας»: περιστατικό το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη·

8) «χειρισμός περιστατικών»: κάθε ενέργεια και διαδικασία που αποσκοπεί στην πρόληψη, τη διαπίστωση, την ανάλυση και τον περιορισμό ή την αντίδραση σε περιστατικό και την ανάκαμψη από αυτό·

9) «κίνδυνος»: η πιθανότητα απώλειας ή διατάραξης που προκαλείται από περιστατικό και εκφράζεται ως συνδυασμός του μεγέθους της εν λόγω απώλειας ή διατάραξης και της πιθανότητας επέλευσης του εν λόγω περιστατικού·

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

11) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή η οποία, βάσει των τεχνικών χαρακτηριστικών της, μπορεί να θεωρηθεί ότι έχει τη δυνατότητα να επηρεάσει σοβαρά τα συστήματα δικτύου και πληροφοριών μιας οντότητας ή των χρηστών υπηρεσιών της οντότητας προκαλώντας σημαντική υλική ή μη υλική ζημία·

12) «προϊόν ΤΠΕ»: προϊόν ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 12) του κανονισμού (ΕΕ) 2019/881·

13) «υπηρεσία ΤΠΕ»: υπηρεσία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 13) του κανονισμού (ΕΕ) 2019/881·

14) «διαδικασία ΤΠΕ»: διαδικασία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 14) του κανονισμού (ΕΕ) 2019/881·

15) «ευπάθεια»: αδυναμία, ευαισθησία ή ελάττωμα προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή·

16) «πρότυπο»: πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([29])·

17) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή όπως ορίζεται στο άρθρο 2 σημείο 4) του κανονισμού (ΕΕ) αριθ. 1025/2012·

([29]) 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).

18) «σημείο ανταλλαγής κίνησης διαδικτύου»: δικτυακή διευκόλυνση που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων δικτύων (αυτόνομων συστημάτων), κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης στο διαδίκτυο, η οποία παρέχει διασύνδεση μόνο για αυτόνομα συστήματα και η οποία ούτε απαιτεί η κυκλοφορία στο διαδίκτυο που διέρχεται μεταξύ οποιουδήποτε ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέρχεται μέσω οποιουδήποτε τρίτου αυτόνομου συστήματος ούτε μεταβάλλει ή επηρεάζει με άλλο τρόπο την εν λόγω κίνηση·

19) «σύστημα ονομάτων χώρου» ή «DNS»: ιεραρχικό κατανεμημένο σύστημα ονοματοδοσίας που επιτρέπει τον προσδιορισμό των διαδικτυακών υπηρεσιών και πόρων, επιτρέποντας στις συσκευές των τελικών χρηστών να χρησιμοποιούν υπηρεσίες δρομολόγησης και συνδεσιμότητας στο διαδίκτυο για την πρόσβαση στις εν λόγω υπηρεσίες και πόρους·

20) «πάροχος υπηρεσιών DNS»: οντότητα που παρέχει:

α) δημόσια διαθέσιμες υπηρεσίες αναδρομικής επίλυσης ονομάτων τομέα για τελικούς χρήστες του διαδικτύου· ή

β) έγκυρες υπηρεσίες επίλυσης ονομάτων τομέα για χρήση από τρίτους, με εξαίρεση τους εξυπηρετητές ονομάτων ρίζας·

21) «μητρώο ονομάτων τομέα ανωτάτου επιπέδου» ή «μητρώο ονομάτων TLD»: οντότητα στην οποία έχει ανατεθεί συγκεκριμένος TLD και είναι υπεύθυνη για τη διαχείριση του TLD, συμπεριλαμβανομένης της καταχώρισης ονομάτων τομέα στο πλαίσιο του TLD και της τεχνικής λειτουργίας του TLD, συμπεριλαμβανομένης της λειτουργίας των εξυπηρετητών ονομάτων του, της συντήρησης των βάσεων δεδομένων του και της διανομής αρχείων ζώνης TLD σε διακομιστές ονομάτων, ανεξάρτητα από το αν οποιαδήποτε από τις εν λόγω πράξεις εκτελείται από την ίδια την οντότητα ή ανατίθεται εξωτερικά, αλλά εξαιρουμένων των περιπτώσεων στις οποίες τα ονόματα TLD χρησιμοποιούνται από μητρώο μόνο για δική της χρήση·

22) «οντότητα που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα»: καταχωρητής ή αντιπρόσωπος που ενεργεί για λογαριασμό καταχωρητών, όπως πάροχος υπηρεσιών καταχώρισης δεδομένων προσωπικού χαρακτήρα ή πληρεξούσιος ή μεταπωλητής·

23) «ψηφιακή υπηρεσία»: υπηρεσία όπως ορίζεται στο άρθρο 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([30])·

24) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή όπως ορίζεται στο άρθρο 3 σημείο 16) του κανονισμού (ΕΕ) αριθ. 910/2014·

25) «πάροχος υπηρεσιών εμπιστοσύνης»: πάροχος υπηρεσιών εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 19) του κανονισμού (ΕΕ) αριθ. 910/2014·

26) «εγκεκριμένη υπηρεσία εμπιστοσύνης»: εγκεκριμένη υπηρεσία εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 17) του κανονισμού (ΕΕ) αριθ. 910/2014·

27) «εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης»: εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης όπως ορίζεται στο άρθρο 3 σημείο 20) του κανονισμού (ΕΕ) αριθ. 910/2014·

28) «επιγραμμική αγορά»: επιγραμμική αγορά όπως ορίζεται στο άρθρο 2 στοιχείο ιδ) της οδηγίας 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([31])·

29) «επιγραμμική μηχανή αναζήτησης»: επιγραμμική μηχανή αναζήτησης όπως ορίζεται στο άρθρο 2 σημείο 5) του κανονισμού (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([32])·

30) «υπηρεσία υπολογιστικού νέφους»: ψηφιακή υπηρεσία που καθιστά δυνατή τη διαχείριση κατά παραγγελία και την ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενη και ελαστική δεξαμενή κοινών υπολογιστικών πόρων, μεταξύ άλλων όταν οι πόροι αυτοί κατανέμονται σε διάφορα σημεία·

([30]) 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).

([31]) Οδηγία 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2005, για τις αθέμιτες εμπορικές πρακτικές των επιχειρήσεων προς τους καταναλωτές στην εσωτερική αγορά και για την τροποποίηση της οδηγίας 84/450/ΕΟΚ του Συμβουλίου, των οδηγιών 97/7/ΕΚ, 98/27/ΕΚ, 2002/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («Οδηγία για τις αθέμιτες εμπορικές πρακτικές») (ΕΕ L 149 της 11.6.2005, σ. 22).

([32]) Κανονισμός (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, για την προώθηση της δίκαιης μεταχείρισης και της διαφάνειας για τους επιχειρηματικούς χρήστες επιγραμμικών υπηρεσιών διαμεσολάβησης (ΕΕ L 186 της 11.7.2019, σ. 57).

31) «υπηρεσία κέντρου δεδομένων»: υπηρεσία που περιλαμβάνει δομές, ή ομάδες δομών, οι οποίες προορίζονται για την κεντρική φιλοξενία, διασύνδεση και λειτουργία εξοπλισμού ΤΠ και δικτύων και παρέχουν υπηρεσίες αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων, καθώς και όλες τις εγκαταστάσεις και υποδομές διανομής ισχύος και περιβαλλοντικού ελέγχου·

32) «δίκτυο διανομής περιεχομένου»: δίκτυο γεωγραφικά κατανεμημένων εξυπηρετητών που αποσκοπεί στη διασφάλιση υψηλής διαθεσιμότητας και προσβασιμότητας ή ταχείας παράδοσης ψηφιακού περιεχομένου και ψηφιακών υπηρεσιών στους χρήστες του διαδικτύου για λογαριασμό παρόχων περιεχομένου και υπηρεσιών·

33) «πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης»: πλατφόρμα που επιτρέπει στους τελικούς χρήστες να συνδέονται, να ανταλλάσσουν, να ανακαλύπτουν και να επικοινωνούν μεταξύ τους μέσω πολλαπλών συσκευών, ιδίως μέσω συνομιλιών, αναρτήσεων, βίντεο και συστάσεων·

34) «εκπρόσωπος»: φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση που έχει οριστεί ρητά να ενεργεί εξ ονόματος παρόχου υπηρεσιών DNS, μητρώου ονομάτων TLD, οντότητας που παρέχει υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχου υπηρεσιών υπολογιστικού νέφους, παρόχου υπηρεσιών κέντρου δεδομένων, παρόχου δικτύου διανομής περιεχομένου, παρόχου διαχειριζομένων υπηρεσιών, παρόχου διαχειριζομένων υπηρεσιών ασφάλειας, παρόχου επιγραμμικής αγοράς, επιγραμμικής μηχανής αναζήτησης ή πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης που δεν είναι εγκατεστημένος στην Ένωση, στον οποίο μπορεί να απευθύνεται αρμόδια αρχή ή CSIRT αντί της ίδιας της οντότητας όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας δυνάμει της παρούσας οδηγίας·

35) «οντότητα δημόσιας διοίκησης»: οντότητα που αναγνωρίζεται ως τέτοια σε κράτος μέλος σύμφωνα με το εθνικό δίκαιο, μη συμπεριλαμβανομένων των δικαστηρίων, των κοινοβουλίων ή των κεντρικών τραπεζών, η οποία πληροί τα ακόλουθα κριτήρια:

α) έχει συσταθεί με σκοπό την κάλυψη αναγκών γενικού συμφέροντος και δεν έχει βιομηχανικό ή εμπορικό χαρακτήρα·

β) έχει νομική προσωπικότητα ή δικαιούται εκ του νόμου να ενεργεί για λογαριασμό άλλης οντότητας με νομική προσωπικότητα·

γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου, υπόκειται σε έλεγχο διαχείρισης από τις εν λόγω αρχές ή οργανισμούς ή έχει διοικητικό, διευθυντικό ή εποπτικό συμβούλιο, του οποίου περισσότερα από τα μισά μέλη διορίζονται από το κράτος, τις περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου·

δ) έχει την εξουσία να απευθύνει σε φυσικά ή νομικά πρόσωπα διοικητικές ή κανονιστικές αποφάσεις που επηρεάζουν τα δικαιώματά τους στη διασυνοριακή κυκλοφορία προσώπων, αγαθών, υπηρεσιών ή κεφαλαίων·

36) «δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών»: δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών, όπως ορίζεται στο άρθρο 2 σημείο 8) της οδηγίας (ΕΕ) 2018/1972·

37) «υπηρεσία ηλεκτρονικών επικοινωνιών»: υπηρεσία ηλεκτρονικών επικοινωνιών, όπως ορίζεται στο άρθρο 2 σημείο 4) της οδηγίας (ΕΕ) 2018/1972·

38) «οντότητα»: φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο βάσει του εθνικού δικαίου του τόπου εγκατάστασής του, το οποίο μπορεί, ενεργώντας για ίδιο λογαριασμό, να ασκεί δικαιώματα και να υπόκειται σε υποχρεώσεις·

39) «πάροχος διαχειριζόμενων υπηρεσιών»: οντότητα που παρέχει υπηρεσίες σχετικές με την εγκατάσταση, τη διαχείριση, τη λειτουργία ή τη συντήρηση προϊόντων, δικτύων, υποδομών, εφαρμογών ΤΠΕ ή οποιωνδήποτε άλλων συστημάτων δικτύου και πληροφοριών, μέσω συνδρομής ή ενεργού διαχείρισης που εκτελείται είτε στις εγκαταστάσεις των πελατών είτε εξ αποστάσεως·

40) «πάροχος διαχειριζόμενων υπηρεσιών ασφάλειας»: πάροχος διαχειριζόμενων υπηρεσιών που εκτελεί ή παρέχει υποστήριξη για δραστηριότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας·

41) «ερευνητικός οργανισμός»: οντότητα που έχει ως πρωταρχικό στόχο τη διεξαγωγή εφαρμοσμένης έρευνας ή πειραματικής ανάπτυξης με σκοπό την εκμετάλλευση των αποτελεσμάτων της εν λόγω έρευνας για εμπορικούς σκοπούς, αλλά η οποία δεν περιλαμβάνει εκπαιδευτικά ιδρύματα.

ΚΕΦΑΛΑΙΟ II

ΣΥΝΤΟΝΙΣΜΕΝΑ ΚΑΝΟΝΙΣΤΙΚΑ ΠΛΑΙΣΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 7

Εθνική στρατηγική κυβερνοασφάλειας

1. Κάθε κράτος μέλος θεσπίζει εθνική στρατηγική κυβερνοασφάλειας που προβλέπει τους στρατηγικούς στόχους, τους πόρους που απαιτούνται για την επίτευξη των εν λόγω στόχων και κατάλληλα μέτρα πολιτικής και ρυθμιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας. Η εθνική στρατηγική κυβερνοασφάλειας περιλαμβάνει:

α) στόχους και προτεραιότητες της στρατηγικής κυβερνοασφάλειας του κράτους μέλους που καλύπτουν ιδίως τους τομείς που αναφέρονται στα παραρτήματα I και II·

β) πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων που αναφέρονται στο στοιχείο α) της παρούσας παραγράφου, συμπεριλαμβανομένων των πολιτικών που αναφέρονται στην παράγραφο 2·

γ) πλαίσιο διακυβέρνησης που αποσαφηνίζει τους ρόλους και τις αρμοδιότητες των σχετικών ενδιαφερόμενων μερών σε εθνικό επίπεδο, το οποίο υποστηρίζει τη συνεργασία και τον συντονισμό σε εθνικό επίπεδο μεταξύ των αρμόδιων αρχών, των ενιαίων κέντρων επαφής και των CSIRT, δυνάμει της παρούσας οδηγίας, καθώς και τον συντονισμό και τη συνεργασία μεταξύ των εν λόγω φορέων και των αρμόδιων αρχών βάσει τομεακών νομικών πράξεων της Ένωσης·

δ) μηχανισμό για τον προσδιορισμό των σχετικών πάγιων στοιχείων και εκτίμηση των κινδύνων στο εν λόγω κράτος μέλος·

ε) προσδιορισμό των μέτρων για τη διασφάλιση της ετοιμότητας, της απόκρισης και της αποκατάστασης από περιστατικά, συμπεριλαμβανομένης της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα·

στ) κατάλογο των διαφόρων αρχών και ενδιαφερόμενων μερών που συμμετέχουν στην εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας·

ζ) πλαίσιο πολιτικής για ενισχυμένο συντονισμό μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και των αρμόδιων αρχών που προβλέπονται στην οδηγία (ΕΕ) 2022/2557, για τον σκοπό της ανταλλαγής πληροφοριών σχετικά με κινδύνους, κυβερνοαπειλές και περιστατικά, καθώς και σχετικά με κινδύνους, απειλές και περιστατικά εκτός κυβερνοχώρου, και την άσκηση εποπτικών καθηκόντων, κατά περίπτωση·

η) σχέδιο, συμπεριλαμβανομένων των αναγκαίων μέτρων, για την ενίσχυση του γενικού επιπέδου ευαισθητοποίησης των πολιτών στον τομέα της κυβερνοασφάλειας.

2. Στο πλαίσιο της εθνικής στρατηγικής κυβερνοασφάλειας, τα κράτη μέλη θεσπίζουν ιδίως πολιτικές:

α) αντιμετώπισης της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού προϊόντων ΤΠΕ και υπηρεσιών ΤΠΕ που χρησιμοποιούνται από οντότητες για την παροχή των υπηρεσιών τους·

β) σχετικά με τη συμπερίληψη και τον προσδιορισμό των σχετικών με την κυβερνοασφάλεια απαιτήσεων για τα προϊόντα ΤΠΕ και τις υπηρεσίες ΤΠΕ στις δημόσιες συμβάσεις, συμπεριλαμβανομένων των σχετικών με την πιστοποίηση της κυβερνοασφάλειας, την κρυπτογράφηση και τη χρήση προϊόντων κυβερνοασφάλειας ανοικτού κώδικα·

γ) διαχείρισης ευπαθειών, συμπεριλαμβανομένης της προώθησης και της διευκόλυνσης της συντονισμένης γνωστοποίησης τρωτοτήτων δυνάμει του άρθρου 12 παράγραφος 1·

δ) σχετικές με τη διατήρηση της γενικής διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητας του δημόσιου πυρήνα του ανοικτού διαδικτύου, συμπεριλαμβανομένης, κατά περίπτωση, της κυβερνοασφάλειας των υποβρύχιων καλωδίων επικοινωνιών·

ε) προώθησης της ανάπτυξης και της ενσωμάτωσης σχετικών προηγμένων τεχνολογιών με στόχο την εφαρμογή προηγμένων μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

στ) προώθησης και ανάπτυξης της εκπαίδευσης και της κατάρτισης στην κυβερνοασφάλεια, τις δεξιότητες κυβερνοασφάλειας, την ευαισθητοποίηση και τις πρωτοβουλίες έρευνας και ανάπτυξης, καθώς και καθοδήγηση σχετικά με ορθές πρακτικές και ελέγχους κυβερνοϋγιεινής, με στόχο τους πολίτες, τα ενδιαφερόμενα μέρη και τις οντότητες·

ζ) στήριξης ακαδημαϊκών και ερευνητικών ιδρυμάτων για την ανάπτυξη, την ενίσχυση και την προώθηση της ανάπτυξης εργαλείων κυβερνοασφάλειας και ασφαλών υποδομών δικτύου·

η) συμπερίληψης σχετικών διαδικασιών και κατάλληλων εργαλείων ανταλλαγής πληροφοριών για τη στήριξη της εθελοντικής ανταλλαγής πληροφοριών για την κυβερνοασφάλεια μεταξύ οντοτήτων σύμφωνα με το δίκαιο της Ένωσης·

θ) ενίσχυσης της κυβερνοανθεκτικότητας και της βάσης για την κυβερνοϋγιεινή των μικρών και μεσαίων επιχειρήσεων, ιδίως εκείνων που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας, με την παροχή εύκολα προσβάσιμης καθοδήγησης και συνδρομής για τις ειδικές ανάγκες τους·

ι) προώθησης της ενεργητικής κυβερνοπροστασίας.

3. Τα κράτη μέλη κοινοποιούν τις εθνικές στρατηγικές κυβερνοασφάλειας στην Επιτροπή εντός τριών μηνών από την έγκρισή τους. Τα κράτη μέλη μπορούν να εξαιρούν από τις εν λόγω κοινοποιήσεις τις πληροφορίες που αφορούν την εθνική τους ασφάλεια.

4. Τα κράτη μέλη αξιολογούν τις εθνικές στρατηγικές κυβερνοασφάλειας σε τακτική βάση και τουλάχιστον ανά πενταετία με βάση βασικούς δείκτες επιδόσεων και, όπου απαιτείται, τους επικαιροποιούν. Ο ENISA επικουρεί τα κράτη μέλη, κατόπιν αιτήματός τους, στην ανάπτυξη ή την επικαιροποίηση εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο και βασικών δεικτών επιδόσεων για την αξιολόγηση της εν λόγω στρατηγικής, με σκοπό την ευθυγράμμισή της με τις απαιτήσεις και τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

Άρθρο 8

Αρμόδιες αρχές και ενιαία σημεία επαφής

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα που αναφέρονται στο κεφάλαιο VII (αρμόδιες αρχές).

2. Οι αρμόδιες αρχές που αναφέρονται στην παράγραφο 1 παρακολουθούν την εφαρμογή της παρούσας οδηγίας σε εθνικό επίπεδο.

3. Κάθε κράτος μέλος ορίζει ή συστήνει ένα ή περισσότερα σημεία επαφής. Όταν ένα κράτος μέλος ορίζει ή συστήνει μόνο μία αρμόδια αρχή σύμφωνα με την παράγραφο 1, η εν λόγω αρμόδια αρχή αποτελεί επίσης το ενιαίο σημείο επαφής για το εν λόγω κράτος μέλος.

4. Κάθε ενιαίο σημείο επαφής ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών του κράτους μέλους του με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Επιτροπή και τον ENISA, καθώς και για τη διασφάλιση διατομεακής συνεργασίας με άλλες αρμόδιες αρχές εντός του οικείου κράτους μέλους.

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους διαθέτουν τις απαιτούμενες εξουσίες και επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους ανατίθενται και να επιτυγχάνουν, με τον τρόπο αυτό, τους στόχους του παρόντος κανονισμού.

6. Κάθε κράτος μέλος κοινοποιεί αμελλητί στην Επιτροπή την ταυτότητα της αρμόδιας αρχής της παραγράφου 1 και του ενιαίου σημείου επαφής της παραγράφου 3, τα καθήκοντα των εν λόγω αρχών, καθώς και κάθε μεταγενέστερη τροποποίηση. Κάθε κράτος μέλος δημοσιοποιεί την ταυτότητα της αρμόδιας αρχής του. Η Επιτροπή δημοσιοποιεί κατάλογο των ενιαίων σημείων επαφής.

Άρθρο 9

Εθνικά πλαίσια διαχείρισης κυβερνοκρίσεων

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας (αρχές διαχείρισης κυβερνοκρίσεων). Τα κράτη μέλη διασφαλίζουν ότι οι οικείες αρμόδιες αρχές διαθέτουν επαρκείς πόρους για την αποτελεσματική και αποδοτική εκτέλεση των καθηκόντων που τους ανατίθενται. Τα κράτη μέλη διασφαλίζουν τη συνοχή με τα υφιστάμενα πλαίσια για τη γενική εθνική διαχείριση κρίσεων.

2. Όταν ένα κράτος μέλος ορίζει ή συστήνει περισσότερες από μία αρχές διαχείρισης κυβερνοκρίσεων σύμφωνα με την παράγραφο 1, αναφέρει σαφώς ποια από τις εν λόγω αρχές θα λειτουργεί ως συντονιστής στη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας.

3. Κάθε κράτος μέλος προσδιορίζει τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν στην περίπτωση κρίσης για τους σκοπούς της παρούσας οδηγίας.

4. Κάθε κράτος μέλος θεσπίζει εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας. Το εν λόγω σχέδιο καθορίζει ιδίως:

α) τους στόχους των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας·

β) τα καθήκοντα και τις αρμοδιότητες των αρχών διαχείρισης κυβερνοκρίσεων·

γ) τις διαδικασίες διαχείρισης κυβερνοκρίσεων, συμπεριλαμβανομένης της ενσωμάτωσής τους στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων και στους διαύλους ανταλλαγής πληροφοριών·

δ) τα εθνικά μέτρα ετοιμότητας, συμπεριλαμβανομένων ασκήσεων και δραστηριοτήτων κατάρτισης·

ε) τα σχετικά ενδιαφερόμενα μέρη δημόσιου και ιδιωτικού τομέα και τις σχετικές υποδομές·

στ) τις εθνικές διαδικασίες και ρυθμίσεις μεταξύ των αρμόδιων εθνικών αρχών και φορέων για να διασφαλίζεται η αποτελεσματική συμμετοχή και η παροχή υποστήριξης εκ μέρους του κράτους μέλους στη συντονισμένη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης.

5. Εντός τριών μηνών από τον ορισμό ή τη σύσταση της αρχής διαχείρισης κυβερνοκρίσεων που αναφέρεται στην παράγραφο 1, κάθε κράτος μέλος κοινοποιεί στην Επιτροπή την ταυτότητα της αρμόδιας αρχής του και τυχόν μεταγενέστερες αλλαγές. Τα κράτη μέλη υποβάλλουν στην Επιτροπή και στο ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις (EU-CyCLONe) σχετικές πληροφορίες σχετικά με τις απαιτήσεις της παραγράφου 4 όσον αφορά τα εθνικά σχέδια αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας εντός τριών μηνών από την έγκριση των εν λόγω σχεδίων. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες πληροφορίες όταν και στον βαθμό που η εξαίρεση αυτή είναι αναγκαία για την εθνική τους ασφάλεια.

Άρθρο 10

Ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)

1. Κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες CSIRT. Οι CSIRT μπορούν να ορίζονται ή να συστήνονται στο πλαίσιο αρμόδιας αρχής. Οι CSIRT συμμορφώνονται με τις απαιτήσεις που ορίζονται στο άρθρο 11 παράγραφος 1, καλύπτουν τουλάχιστον τους τομείς, τους υποτομείς και τους τύπους οντοτήτων που αναφέρονται στα παραρτήματα I και II και είναι υπεύθυνες για τον χειρισμό περιστατικών σύμφωνα με σαφώς καθορισμένη διαδικασία.

2. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει επαρκείς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων της, όπως ορίζονται στο άρθρο 11 παράγραφος 3.

3. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει κατάλληλη, ασφαλή και ανθεκτική υποδομή επικοινωνίας και πληροφοριών μέσω της οποίας ανταλλάσσει πληροφορίες με βασικές και σημαντικές οντότητες και άλλα σχετικά ενδιαφερόμενα μέρη. Για τον σκοπό αυτό, τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT συμβάλλει στην ανάπτυξη ασφαλών εργαλείων ανταλλαγής πληροφοριών.

4. Οι CSIRT συνεργάζονται και, κατά περίπτωση, ανταλλάσσουν σχετικές πληροφορίες σύμφωνα με το άρθρο 29 με τομεακές ή διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων.

5. Οι CSIRT συμμετέχουν σε αξιολογήσεις από ομοτίμους που διοργανώνονται σύμφωνα με το άρθρο 19.

6. Τα κράτη μέλη διασφαλίζουν την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των CSIRT τους στο δίκτυο CSIRT.

7. Οι CSIRT μπορούν να συνάπτουν σχέσεις συνεργασίας με τις εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας. Στο πλαίσιο αυτών των σχέσεων συνεργασίας, τα κράτη μέλη διευκολύνουν την αποτελεσματική, αποδοτική και ασφαλή ανταλλαγή πληροφοριών με τις εν λόγω εθνικές ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές τρίτης χώρας, χρησιμοποιώντας σχετικά πρωτόκολλα ανταλλαγής πληροφοριών, συμπεριλαμβανομένου του πρωτοκόλλου φωτεινού σηματοδότη. Οι CSIRT μπορούν να ανταλλάσσουν σχετικές πληροφορίες με εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας, συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων.

8. Οι CSIRT μπορούν να συνεργάζονται με εθνικές ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές τρίτης χώρας ή με ισοδύναμους φορείς τρίτης χώρας, ιδίως με σκοπό την παροχή συνδρομής στον τομέα της κυβερνοασφάλειας.

9. Κάθε κράτος μέλος κοινοποιεί αμελλητί στην Επιτροπή την ταυτότητα της CSIRT που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου και της CSIRT στην οποία έχουν ανατεθεί καθήκοντα συντονισμού σύμφωνα με το άρθρο 12 παράγραφος 1, τα αντίστοιχα καθήκοντά τους σε σχέση με βασικές και σημαντικές οντότητες, και τυχόν μεταγενέστερες αλλαγές τους.

10. Τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του ENISA για την ανάπτυξη των CSIRT τους.

Άρθρο 11

Απαιτήσεις, τεχνικές ικανότητες και καθήκοντα των CSIRT

1. Οι CSIRT συμμορφώνονται με τις ακόλουθες απαιτήσεις:

α) οι CSIRT εξασφαλίζουν υψηλό επίπεδο διαθεσιμότητας των διαύλων επικοινωνίας τους αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτουν διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. προσδιορίζουν σαφώς τους διαύλους επικοινωνίας και τους γνωστοποιούν στα μέλη της περιοχής ευθύνης τους και στους συνεργαζόμενους εταίρους·

β) οι εγκαταστάσεις των CSIRT και τα υποστηρικτικά πληροφοριακά συστήματα βρίσκονται σε ασφαλείς χώρους·

γ) οι CSIRT είναι εφοδιασμένες με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, ιδίως προκειμένου να διευκολύνεται η αποτελεσματική και αποδοτική παράδοση καθηκόντων·

δ) οι CSIRT διασφαλίζουν την εμπιστευτικότητα και την αξιοπιστία των δραστηριοτήτων τους·

ε) οι CSIRT είναι επαρκώς στελεχωμένες ώστε να διασφαλίζουν τη διαθεσιμότητα των υπηρεσιών τους ανά πάσα στιγμή και διασφαλίζουν ότι το προσωπικό τους είναι κατάλληλα καταρτισμένο·

στ) οι CSIRT είναι εξοπλισμένες με πλεονάζοντα συστήματα και εφεδρικό χώρο εργασίας για τη διασφάλιση της συνέχειας των υπηρεσιών τους.

Οι CSIRT μπορούν να συμμετέχουν σε διεθνή δίκτυα συνεργασίας.

2. Τα κράτη μέλη διασφαλίζουν ότι οι CSIRT τους διαθέτουν από κοινού τις τεχνικές ικανότητες που απαιτούνται για την εκτέλεση των καθηκόντων που αναφέρονται στην παράγραφο 3. Τα κράτη μέλη διασφαλίζουν ότι διατίθενται επαρκείς πόροι στις CSIRT τους ώστε να εξασφαλίζονται επαρκή επίπεδα στελέχωσης για να μπορούν οι CSIRT να αναπτύξουν τις τεχνικές τους ικανότητες.

3. Οι CSIRT είναι επιφορτισμένες με τα ακόλουθα καθήκοντα:

α) παρακολούθηση και ανάλυση κυβερνοαπειλών, ευπαθειών και περιστατικών σε εθνικό επίπεδο και, κατόπιν αιτήματος, παροχή συνδρομής σε επηρεαζόμενες βασικές και σημαντικές οντότητες σχετικά με την παρακολούθηση των συστημάτων δικτύου και πληροφοριών τους σε πραγματικό χρόνο ή σχεδόν σε πραγματικό χρόνο·

β) παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων, ανακοινώσεων και διάδοσης πληροφοριών σε εμπλεκόμενες βασικές και σημαντικές οντότητες, καθώς και σε αρμόδιες αρχές και άλλα σχετικά ενδιαφερόμενα μέρη σχετικά με κυβερνοαπειλές, τρωτότητες και περιστατικά, ει δυνατόν σε σχεδόν πραγματικό χρόνο·

γ) αντιμετώπιση περιστατικών και παροχή συνδρομής στις επηρεαζόμενες βασικές και σημαντικές οντότητες, κατά περίπτωση·

δ) συλλογή και ανάλυση εγκληματολογικών δεδομένων και δυναμική ανάλυση κινδύνων και περιστατικών και επίγνωση της κατάστασης σε θέματα κυβερνοασφάλειας·

ε) παροχή, κατόπιν αιτήματος βασικής ή σημαντικής οντότητας, προληπτικής σάρωσης των συστημάτων δικτύου και πληροφοριών της οικείας οντότητας για τον εντοπισμό ευπαθειών με δυνητικό σημαντικό αντίκτυπο·

στ) συμμετοχή στο δίκτυο CSIRT και παροχή αμοιβαίας συνδρομής σύμφωνα με τις ικανότητες και τις αρμοδιότητές τους σε άλλα μέλη του δικτύου CSIRT κατόπιν αιτήματός τους·

ζ) κατά περίπτωση, ανάληψη συντονιστικού ρόλου για τους σκοπούς της συντονισμένης διαδικασίας γνωστοποίησης τρωτοτήτων δυνάμει του άρθρου 12 παράγραφος 1·

η) συμβολή στην ανάπτυξη ασφαλών εργαλείων ανταλλαγής πληροφοριών σύμφωνα με το άρθρο 10 παράγραφος 3.

Οι CSIRT μπορούν να διενεργούν προληπτική μη παρεμβατική σάρωση των δημοσίως προσβάσιμων συστημάτων δικτύου και πληροφοριών βασικών και σημαντικών οντοτήτων. Η εν λόγω σάρωση διενεργείται για τον εντοπισμό ευπαθών ή επισφαλώς διαμορφωμένων συστημάτων δικτύου και πληροφοριών και για την ενημέρωση των οικείων οντοτήτων. Η εν λόγω σάρωση δεν έχει αρνητικές συνέπειες για τη λειτουργία των υπηρεσιών των οντοτήτων.

Κατά την εκτέλεση των καθηκόντων που αναφέρονται στο πρώτο εδάφιο, οι CSIRT μπορούν να δίνουν προτεραιότητα σε συγκεκριμένα καθήκοντα στο πλαίσιο προσέγγισης βάσει κινδύνου.

4. Οι CSIRT συνάπτουν σχέσεις συνεργασίας με τα σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα, με σκοπό την επίτευξη των στόχων της παρούσας οδηγίας.

5. Προκειμένου να διευκολυνθεί η συνεργασία που αναφέρεται στην παράγραφο 4, οι CSIRT προωθούν την υιοθέτηση και τη χρήση κοινών ή τυποποιημένων πρακτικών, συστημάτων ταξινόμησης και ταξινομιών σε σχέση με:

α) διαδικασίες χειρισμού περιστατικών·

β) διαχείριση κρίσεων· και

γ) συντονισμένη γνωστοποίηση ευπαθειών δυνάμει του άρθρου 12 παράγραφος 1.

Άρθρο 12

Συντονισμένη γνωστοποίηση ευπαθειών και ευρωπαϊκή βάση δεδομένων ευπαθειών

1. Κάθε κράτος μέλος αναθέτει σε μία από τις CSIRT του συντονιστικό ρόλο για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών. Η CSIRT στην οποία ανατίθενται συντονιστικά καθήκοντα ενεργεί ως αξιόπιστος διαμεσολαβητής, διευκολύνοντας, όπου απαιτείται, την αλληλεπίδραση μεταξύ του φυσικού ή νομικού προσώπου που αναφέρει την ευπάθεια και του κατασκευαστή ή του παρόχου των δυνητικά ευπαθών προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ, κατόπιν αιτήματος ενός εκ των μερών. Τα καθήκοντα της CSIRT στην οποία έχει ανατεθεί συντονιστικός ρόλος περιλαμβάνουν:

α) τον προσδιορισμό των οικείων οντοτήτων και την επικοινωνία με αυτές·

β) την παροχή συνδρομής στα φυσικά ή νομικά πρόσωπα που αναφέρουν ευπάθειες· και

γ) τη διαπραγμάτευση χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση ευπαθειών που επηρεάζουν πλείονες οντότητες.

Τα κράτη μέλη διασφαλίζουν ότι τα φυσικά ή νομικά πρόσωπα μπορούν να αναφέρουν ανώνυμα, εφόσον το ζητήσουν, ευπάθειες στην CSIRT στην οποία έχει ανατεθεί ο συντονισμός. Η CSIRT στην οποία έχει ανατεθεί ο συντονισμός διασφαλίζει ότι εκτελούνται επιμελείς ενέργειες παρακολούθησης όσον αφορά την αναφερθείσα τρωτότητα και διασφαλίζει την ανωνυμία του φυσικού ή νομικού προσώπου που αναφέρει την τρωτότητα. Στις περιπτώσεις όπου μια αναφερόμενη ευπάθεια θα μπορούσε να έχει σημαντικό αντίκτυπο σε οντότητες σε περισσότερα του ενός κράτη μέλη, η CSIRT στην οποία έχει ανατεθεί ο συντονισμός σε κάθε ενδιαφερόμενο κράτος μέλος συνεργάζεται, κατά περίπτωση, με άλλες CSIRT στις οποίες έχει ανατεθεί συντονιστικός ρόλος στο πλαίσιο του δικτύου CSIRT.

2. Ο ENISA αναπτύσσει και διατηρεί, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας, ευρωπαϊκή βάση δεδομένων ευπαθειών. Για τον σκοπό αυτό, ο ENISA καταρτίζει και διατηρεί τα κατάλληλα συστήματα πληροφοριών, πολιτικές και διαδικασίες και θεσπίζει τα αναγκαία τεχνικά και οργανωτικά μέτρα για τη διαφύλαξη της ασφάλειας και της ακεραιότητας της ευρωπαϊκής βάσης δεδομένων ευπαθειών, με σκοπό ιδίως να δοθεί η δυνατότητα στις οντότητες, ανεξαρτήτως από το αν εμπίπτουν στο πεδίο της παρούσας οδηγίας, και στους προμηθευτές συστημάτων δικτύου και πληροφοριών τους να δημοσιοποιούν και να καταχωρίζουν, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες σε προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ. Παρέχεται σε όλα τα ενδιαφερόμενα μέρη πρόσβαση στις πληροφορίες σχετικά με τις ευπάθειες που περιέχονται στην ευρωπαϊκή βάση δεδομένων ευπαθειών. Η εν λόγω βάση δεδομένων περιλαμβάνει:

α) πληροφορίες που περιγράφουν την ευπάθεια·

β) τα επηρεαζόμενα προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ και τη σοβαρότητα της ευπάθειας όσον αφορά τις περιστάσεις υπό τις οποίες μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης·

γ) τη διαθεσιμότητα διορθωτικών προγραμμάτων και, ελλείψει διορθωτικών προγραμμάτων, υλικό καθοδήγησης που παρέχεται από τις αρμόδιες αρχές ή CSIRT και απευθύνεται στους χρήστες προϊόντων ΤΠΕ και υπηρεσιών ΤΠΕ που εμφανίζουν την ευπάθεια, σχετικά με τον τρόπο μετριασμού των κινδύνων που απορρέουν από τις γνωστοποιηθείσες ευπάθειες.

Άρθρο 13

Συνεργασία σε εθνικό επίπεδο

1. Εφόσον πρόκειται για διακριτές οντότητες, οι αρμόδιες αρχές, το ενιαίο σημείο επαφής και οι CSIRT του ίδιου κράτους μέλους συνεργάζονται μεταξύ τους για τους σκοπούς της τήρησης των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.

2. Τα κράτη μέλη διασφαλίζουν ότι οι CSIRT ή, κατά περίπτωση, οι αρμόδιες αρχές τους λαμβάνουν αναφορές σοβαρών περιστατικών σύμφωνα με το άρθρο 23, καθώς και περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών σύμφωνα με το άρθρο 30.

3. Κάθε κράτος μέλος μεριμνά ώστε οι CSIRT του ή, κατά περίπτωση, οι αρμόδιες αρχές του να ενημερώνουν τα ενιαία σημεία επαφής τους για κοινοποιήσεις περιστατικών, κυβερνοαπειλών και παρ' ολίγον περιστατικών που υποβάλλονται σύμφωνα με την παρούσα οδηγία.

4. Προκειμένου να διασφαλιστεί η αποτελεσματική εκτέλεση των καθηκόντων και των υποχρεώσεων των αρμόδιων αρχών, των ενιαίων σημείων επαφής, και των CSIRT, τα κράτη μέλη διασφαλίζουν, στο μέτρο του δυνατού, την κατάλληλη συνεργασία μεταξύ των εν λόγω φορέων και των αρχών επιβολής του νόμου, των αρχών προστασίας δεδομένων, των εθνικών αρχών δυνάμει των κανονισμών (ΕΚ) αριθ. 300/2008 και (ΕΕ) 2018/1139, των εποπτικών φορέων δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, των αρμόδιων αρχών δυνάμει του κανονισμού (ΕΕ) 2022/2554, των εθνικών ρυθμιστικών αρχών δυνάμει της οδηγίας (ΕΕ) 2018/1972, των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) 2022/2557, καθώς και των αρμόδιων αρχών βάσει άλλων τομεακών νομικών πράξεων της Ένωσης, εντός του εν λόγω κράτους μέλους.

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές τους δυνάμει της οδηγίας (ΕΕ) 2022/2557 συνεργάζονται και ανταλλάσσουν πληροφορίες σε τακτική βάση όσον αφορά τον προσδιορισμό των κρίσιμων οντοτήτων, τους κινδύνους, τις κυβερνοαπειλές και τα περιστατικά, καθώς και τους κινδύνους, τις απειλές και τα περιστατικά εκτός του κυβερνοχώρου, που επηρεάζουν βασικές οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557, και τα μέτρα που λαμβάνονται για την αντιμετώπιση των εν λόγω κινδύνων, απειλών και περιστατικών. Τα κράτη μέλη διασφαλίζουν επίσης ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας και οι αρμόδιες αρχές τους δυνάμει του κανονισμού (ΕΕ) αριθ. 910/2014, του κανονισμού (ΕΕ) 2022/2554 και της οδηγίας (ΕΕ) 2018/1972 ανταλλάσσουν σχετικές πληροφορίες σε τακτική βάση, μεταξύ άλλων όσον αφορά συναφή περιστατικά και κυβερνοαπειλές.

6. Τα κράτη μέλη απλουστεύουν την υποβολή αναφορών με τεχνικά μέσα για τις κοινοποιήσεις που αναφέρονται στα άρθρα 23 και 30.

ΚΕΦΑΛΑΙΟ III

ΣΥΝΕΡΓΑΣΙΑ ΣΕ ΕΝΩΣΙΑΚΟ ΚΑΙ ΔΙΕΘΝΕΣ ΕΠΙΠΕΔΟ

Άρθρο 14

Ομάδα Συνεργασίας

1. Για την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, καθώς και την ενίσχυση της πίστης και της εμπιστοσύνης, συστήνεται Ομάδα Συνεργασίας.

2. Η Ομάδα Συνεργασίας εκτελεί τα καθήκοντά της βάσει διετών προγραμμάτων εργασιών τα οποία αναφέρονται στην παράγραφο 7.

3. Η Ομάδα Συνεργασίας απαρτίζεται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA. Η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης συμμετέχει στις δραστηριότητες της ομάδας συνεργασίας ως παρατηρητής. Οι Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) και οι αρμόδιες αρχές δυνάμει του κανονισμού (ΕΕ) 2022/2554 μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας σύμφωνα με το άρθρο 47 παράγραφος 1 του εν λόγω κανονισμού.

Όποτε είναι σκόπιμο, η Ομάδα Συνεργασίας μπορεί να καλεί εκπροσώπους του Ευρωπαϊκού Κοινοβουλίου και σχετικών ενδιαφερόμενων μερών για να συμμετάσχουν στις εργασίες της.

Η Επιτροπή παρέχει τη γραμματειακή υποστήριξη.

4. Τα καθήκοντα της Ομάδας Συνεργασίας είναι τα εξής:

α) παροχή καθοδήγησης στις αρμόδιες αρχές όσον αφορά τη μεταφορά στο εθνικό δίκαιο και την εφαρμογή της παρούσας οδηγίας·

β) παροχή καθοδήγησης στις αρμόδιες αρχές σε σχέση με την ανάπτυξη και την εφαρμογή πολιτικών για τη συντονισμένη γνωστοποίηση ευπαθειών, όπως αναφέρεται στο άρθρο 7 παράγραφος 2 στοιχείο γ)·

γ) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σχετικά με την εφαρμογή της παρούσας οδηγίας, μεταξύ άλλων όσον αφορά κυβερνοαπειλές, περιστατικά, ευπάθειες, παρ' ολίγον περιστατικά, πρωτοβουλίες ευαισθητοποίησης, προγράμματα κατάρτισης, ασκήσεις και δεξιότητες, ανάπτυξη ικανοτήτων, προτύπων και τεχνικών προδιαγραφών, καθώς και τον προσδιορισμό βασικών και σημαντικών οντοτήτων βάσει του άρθρου 2 παράγραφος 2 στοιχεία β) έως ε)·

δ) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με αναδυόμενες πρωτοβουλίες πολιτικής σε θέματα κυβερνοασφάλειας και τη συνολική συνεκτικότητα των ειδικών ανά τομέα απαιτήσεων κυβερνοασφάλειας·

ε) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με σχέδια εκτελεστικών πράξεων που εκδίδονται δυνάμει της παρούσας οδηγίας·

στ) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών με τα αρμόδια θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

ζ) ανταλλαγή απόψεων σχετικά με την εφαρμογή τομεακών νομικών πράξεων της Ένωσης που περιέχουν διατάξεις για την κυβερνοασφάλεια·

η) κατά περίπτωση, εξέταση των εκθέσεων σχετικά με την αξιολόγηση από ομοτίμους που αναφέρεται στο άρθρο 19 παράγραφος 9 και σύνταξη συμπερασμάτων και συστάσεων·

θ) διεξαγωγή συντονισμένων εκτιμήσεων κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού σύμφωνα με το άρθρο 22 παράγραφος 1·

ι) εξέταση περιπτώσεων αμοιβαίας συνδρομής, συμπεριλαμβανομένων εμπειριών και αποτελεσμάτων από διασυνοριακές κοινές εποπτικές δράσεις όπως αναφέρεται στο άρθρο 37·

ια) κατόπιν αιτήματος ενός ή περισσότερων ενδιαφερόμενων κρατών μελών, εξέταση συγκεκριμένων αιτήσεων αμοιβαίας συνδρομής που αναφέρονται στο άρθρο 37·

ιβ) παροχή στρατηγικής καθοδήγησης στο δίκτυο CSIRT και στην EU-CyCLONe σχετικά με συγκεκριμένα αναδυόμενα ζητήματα·

ιγ) ανταλλαγή απόψεων σχετικά με την πολιτική για τις δράσεις παρακολούθησης μετά από περιστατικά μεγάλης κλίμακας και κρίσεις, στον τομέα της κυβερνοασφάλειας με βάση τα διδάγματα που αντλήθηκαν από το δίκτυο CSIRT και την EU-CyCLONe·

ιδ) συμβολή στις ικανότητες κυβερνοασφάλειας σε ολόκληρη την Ένωση, διευκολύνοντας την ανταλλαγή εθνικών υπαλλήλων μέσω προγράμματος ανάπτυξης ικανοτήτων με τη συμμετοχή προσωπικού από τις αρμόδιες αρχές ή τις CSIRT·

ιε) διοργάνωση τακτικών κοινών συνεδριάσεων με σχετικά ενδιαφερόμενα μέρη του ιδιωτικού τομέα από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που πραγματοποιεί η Ομάδα Συνεργασίας και τη συγκέντρωση στοιχείων σχετικά με αναδυόμενες προκλήσεις πολιτικής·

ιστ) εξέταση του έργου που έχει αναληφθεί σε σχέση με τις ασκήσεις κυβερνοασφάλειας, συμπεριλαμβανομένου του έργου που επιτελεί ο ENISA·

ιζ) καθορισμός της μεθοδολογίας και των οργανωτικών πτυχών των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19 παράγραφος 1, καθώς και της μεθοδολογίας αυτοαξιολόγησης για τα κράτη μέλη σύμφωνα με το άρθρο 19 παράγραφος 5, με τη βοήθεια της Επιτροπής και του ENISA, και, σε συνεργασία με την Επιτροπή και τον ENISA, κατάρτιση κωδίκων δεοντολογίας στους οποίους στηρίζονται οι μέθοδοι εργασίας των ορισθέντων εμπειρογνωμόνων κυβερνοασφάλειας σύμφωνα με το άρθρο 19 παράγραφος 6·

ιη) κατάρτιση εκθέσεων για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 40 σχετικά με την πείρα που αποκτήθηκε σε στρατηγικό επίπεδο και από αξιολογήσεις από ομοτίμους·

ιθ) συζήτηση και τακτική αξιολόγηση της κατάστασης σε σχέση με κυβερνοαπειλές ή περιστατικά, όπως επιθέσεις λυτρισμικού.

Η Ομάδα Συνεργασίας υποβάλλει τις εκθέσεις που αναφέρονται στο πρώτο εδάφιο στοιχείο ιη) στην Επιτροπή, στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

5. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των αντιπροσώπων τους στο πλαίσιο της ομάδας συνεργασίας.

6. Η Ομάδα Συνεργασίας μπορεί να ζητήσει από το δίκτυο CSIRT να εκπονήσει τεχνική έκθεση σχετικά με επιλεγμένα θέματα.

7. Έως την 1η Φεβρουαρίου 2024, και στη συνέχεια ανά διετία, η Ομάδα Συνεργασίας καταρτίζει πρόγραμμα εργασιών σχετικά με τις δράσεις που πρέπει να αναληφθούν για την υλοποίηση των στόχων και των καθηκόντων της.

8. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις που καθορίζουν τις διαδικαστικές ρυθμίσεις που είναι αναγκαίες για τη λειτουργία της Ομάδας Συνεργασίας.

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας σχετικά με τα σχέδια εκτελεστικών πράξεων που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου σύμφωνα με την παράγραφο 4 στοιχείο ε).

9. Η Ομάδα Συνεργασίας συνεδριάζει σε τακτική βάση, και σε κάθε περίπτωση τουλάχιστον μία φορά ετησίως, με την ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων που συστάθηκε βάσει της οδηγίας (ΕΕ) 2022/2557 για την προώθηση και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών.

Άρθρο 15

Δίκτυο CSIRT

1. Δημιουργείται δίκτυο εθνικών CSIRT με σκοπό τη συμβολή στην ανάπτυξη πίστης και εμπιστοσύνης και την προώθηση ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών.

2. Το δίκτυο CSIRT απαρτίζεται από εκπροσώπους των CSIRT που ορίζονται ή συγκροτούνται σύμφωνα με το άρθρο 10 και της Ομάδας Αντιμετώπισης Έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης (CERT-EU). Η Επιτροπή συμμετέχει στο δίκτυο CSIRT ως παρατηρητής. Ο ENISA παρέχει γραμματειακή υποστήριξη και παρέχει ενεργά συνδρομή για τη συνεργασία μεταξύ των CSIRT.

3. Τα καθήκοντα του δικτύου CSIRT είναι τα εξής:

α) ανταλλαγή πληροφοριών σχετικά με τις ικανότητες των CSIRT·

β) διευκόλυνση του διαμοιρασμού, μεταφοράς και ανταλλαγής τεχνολογίας και σχετικών μέτρων, πολιτικών, εργαλείων, διαδικασιών, βέλτιστων πρακτικών και πλαισίων μεταξύ των CSIRT·

γ) ανταλλαγή πληροφοριών σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και ευπάθειες·

δ) ανταλλαγή πληροφοριών σχετικά με δημοσιεύσεις και συστάσεις για την κυβερνοασφάλεια·

ε) εξασφάλιση διαλειτουργικότητας όσον αφορά τις προδιαγραφές και τα πρωτόκολλα ανταλλαγής πληροφοριών·

στ) κατόπιν αιτήματος μέλους του δικτύου CSIRT, το οποίο επηρεάζεται δυνητικά από περιστατικό, ανταλλαγή και συζήτηση πληροφοριών σχετικά με το εν λόγω περιστατικό και τις συναφείς κυβερνοαπειλές, τους κινδύνους και τις ευπάθειες·

ζ) κατόπιν αιτήματος μέλους του δικτύου CSIRT, συζήτηση και, ει δυνατόν, εφαρμογή συντονισμένης αντίδρασης σε περιστατικό που έχει εντοπιστεί εντός της δικαιοδοσίας του εν λόγω κράτους μέλους·

η) παροχή συνδρομής στα κράτη μέλη για την αντιμετώπιση διασυνοριακών περιστατικών σύμφωνα με την παρούσα οδηγία·

θ) συνεργασία, ανταλλαγή βέλτιστων πρακτικών και παροχή βοήθειας στις CSIRT στις οποίες ανατίθεται συντονισμός σύμφωνα με το άρθρο 12 παράγραφος 1 όσον αφορά τη διαχείριση της συντονισμένης δημοσιοποίησης ευπαθειών που θα μπορούσαν να έχουν σημαντικό αντίκτυπο σε οντότητες σε περισσότερα από ένα κράτη μέλη·

ι) συζήτηση και προσδιορισμός περαιτέρω μορφών επιχειρησιακής συνεργασίας, μεταξύ άλλων σε σχέση με:

i) τις κατηγορίες κυβερνοαπειλών και περιστατικών·

ii) τις έγκαιρες προειδοποιήσεις·

iii) την αμοιβαία συνδρομή·

iv) τις αρχές και τις ρυθμίσεις συντονισμού για την αντιμετώπιση διασυνοριακών κινδύνων και περιστατικών·

v) τη συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας που αναφέρεται στο άρθρο 9 παράγραφος 4 κατόπιν αιτήματος κράτους μέλους·

ια) ενημέρωση της Ομάδας Συνεργασίας σχετικά με τις δραστηριότητές του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται σύμφωνα με το στοιχείο ι) και, όπου κρίνεται αναγκαίο, υποβολή σχετικού αιτήματος καθοδήγησης·

ιβ) απολογισμός των ασκήσεων κυβερνοασφάλειας, συμπεριλαμβανομένων εκείνων που διοργανώνει ο ENISA·

ιγ) κατόπιν αιτήματος επιμέρους CSIRT, συζήτηση των ικανοτήτων και της ετοιμότητας του εν λόγω CSIRT·

ιδ) συνεργασία και ανταλλαγή πληροφοριών με περιφερειακά και ενωσιακά κέντρα επιχειρήσεων ασφάλειας (SOCs) με σκοπό τη βελτίωση της κοινής επίγνωσης της κατάστασης σχετικά με περιστατικά και κυβερνοαπειλές σε ολόκληρη την Ένωση·

ιε) κατά περίπτωση, συζήτηση των εκθέσεων αξιολόγησης από ομοτίμους που αναφέρονται στο άρθρο 19 παράγραφος 9·

ιστ) θέσπιση κατευθυντήριων γραμμών προκειμένου να διευκολυνθεί η σύγκλιση των επιχειρησιακών πρακτικών όσον αφορά την εφαρμογή των διατάξεων του παρόντος άρθρου σχετικά με την επιχειρησιακή συνεργασία.

4. Έως τις 17 Ιανουαρίου 2025, και στη συνέχεια ανά διετία, το δίκτυο CSIRT αξιολογεί, για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 40, την πρόοδο που έχει σημειωθεί όσον αφορά την επιχειρησιακή συνεργασία και εγκρίνει έκθεση. Ειδικότερα, η έκθεση διατυπώνει συμπεράσματα και συστάσεις με βάση τα αποτελέσματα των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19, οι οποίες διενεργούνται σε σχέση με τις εθνικές CSIRT. Η εν λόγω έκθεση υποβάλλεται στην Ομάδα Συνεργασίας.

5. Το δίκτυο CSIRT εγκρίνει τον εσωτερικό του κανονισμό.

6. Το δίκτυο CSIRT και η EU-CyCLONe συμφωνούν επί των διαδικαστικών ρυθμίσεων και συνεργάζονται βάσει αυτών.

Άρθρο 16

Ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για κρίσεις στον κυβερνοχώρο (EU-CyCLONe)

1. Το EU-CyCLONe συστήνεται για να στηρίζει τη συντονισμένη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και να διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

2. Το EU-CyCLONe απαρτίζεται από εκπροσώπους των αρχών διαχείρισης κρίσεων στον κυβερνοχώρο των κρατών μελών, καθώς και, σε περιπτώσεις όπου ένα δυνητικό ή εν εξελίξει περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο σε υπηρεσίες και δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, από εκπροσώπους της Επιτροπής. Στις άλλες περιπτώσεις, η Επιτροπή συμμετέχει στις δραστηριότητες του EU-CyCLONe με καθεστώς παρατηρητή.

Ο ENISA παρέχει γραμματειακή υποστήριξη στο EU-CyCLONe και υποστηρίζει την ασφαλή ανταλλαγή πληροφοριών, παρέχει δε επίσης τα απαιτούμενα εργαλεία για τη στήριξη της συνεργασίας μεταξύ των κρατών μελών, διασφαλίζοντας την ασφαλή ανταλλαγή πληροφοριών.

Κατά περίπτωση, το EU-CyCLONe μπορεί να καλεί το Ευρωπαϊκό Κοινοβούλιο και εκπροσώπους των σχετικών ενδιαφερόμενων μερών να συμμετάσχουν στις εργασίες του.

3. Τα καθήκοντα του EU-CyCLONe είναι τα εξής:

α) αύξηση του επιπέδου ετοιμότητας για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας·

β) ανάπτυξη κοινής επίγνωσης της κατάστασης για περιστατικά και κρίσεις μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας·

γ) αξιολόγηση των συνεπειών και του αντικτύπου των σχετικών περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας και υποβολή προτάσεων για πιθανά μέτρα μετριασμού·

δ) συντονισμός της διαχείρισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας και στήριξη της λήψης αποφάσεων σε πολιτικό επίπεδο σε σχέση με τέτοια περιστατικά και κρίσεις·

ε) συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας που αναφέρεται στο άρθρο 9 παράγραφος 4, κατόπιν αιτήματος ενδιαφερόμενου κράτους μέλους.

4. Το δίκτυο EU-CyCLONe θεσπίζει τον εσωτερικό κανονισμό του.

5. Το EU-CyCLONe υποβάλλει τακτικά εκθέσεις στην Ομάδα Συνεργασίας σχετικά με τη διαχείριση των περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, καθώς και τις τάσεις, εστιάζοντας ιδίως στον αντίκτυπό τους στις βασικές και τις σημαντικές οντότητες.

6. Το EU-CyCLONe συνεργάζεται με το δίκτυο CSIRT βάσει συμφωνημένων διαδικαστικών ρυθμίσεων που προβλέπονται στο άρθρο 15 παράγραφος 6.

7. Έως τις 17 Ιουλίου 2024, και στη συνέχεια κάθε 18 μήνες, το EU-CyCLONe υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση αξιολόγησης του έργου του.

Άρθρο 17

Διεθνής συνεργασία

Η Ένωση μπορεί, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς, που επιτρέπουν και οργανώνουν τη συμμετοχή τους σε ορισμένες δραστηριότητες της ομάδας συνεργασίας και του δικτύου CSIRT και του EU-CyCLONe. Οι εν λόγω συμφωνίες συμμορφώνονται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.

Άρθρο 18

Έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση

1. Ο ENISA εκδίδει, σε συνεργασία με την Επιτροπή και την Ομάδα Συνεργασίας, διετή έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση, την οποία υποβάλλει και υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο. Η έκθεση διατίθεται, μεταξύ άλλων, σε μηχαναγνώσιμα δεδομένα και περιλαμβάνει τα εξής:

α) αξιολόγηση κινδύνου κυβερνοασφάλειας σε επίπεδο Ένωσης, λαμβάνοντας υπόψη το τοπίο των κυβερνοαπειλών·

β) αξιολόγηση της ανάπτυξης ικανοτήτων κυβερνοασφάλειας στον δημόσιο και τον ιδιωτικό τομέα σε ολόκληρη την Ένωση·

γ) αξιολόγηση του γενικού επιπέδου ευαισθητοποίησης σε θέματα κυβερνοασφάλειας και κυβερνοϋγιεινής μεταξύ των πολιτών και των οντοτήτων, συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων·

δ) συγκεντρωτική αξιολόγηση των αποτελεσμάτων των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 19·

ε) συγκεντρωτική αξιολόγηση του επιπέδου ωριμότητας των ικανοτήτων και των πόρων κυβερνοασφάλειας σε ολόκληρη την Ένωση, συμπεριλαμβανομένων εκείνων σε τομεακό επίπεδο, καθώς και του βαθμού ευθυγράμμισης των εθνικών στρατηγικών κυβερνοασφάλειας των κρατών μελών.

2. Η έκθεση περιλαμβάνει συγκεκριμένες συστάσεις πολιτικής για την αντιμετώπιση αδυναμιών και την αύξηση του επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση και σύνοψη των ευρημάτων για περιστατικά και κυβερνοαπειλές που αφορούν τη συγκεκριμένη περίοδο από τις τεχνικές εκθέσεις για την κατάσταση της κυβερνοασφάλειας στην ΕΕ που εκδίδει ο ENISA σύμφωνα με το άρθρο 7 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881.

3. Ο ENISA, σε συνεργασία με την Επιτροπή, την Ομάδα Συνεργασίας και το δίκτυο CSIRT, αναπτύσσει τη μεθοδολογία, της συγκεντρωτικής αξιολόγησης που αναφέρεται στην παράγραφο 1 στοιχείο ε), συμπεριλαμβανομένων των σχετικών μεταβλητών, όπως ποσοτικούς και ποιοτικούς δείκτες.

Άρθρο 19

Αξιολογήσεις από ομότιμους

1. Η Ομάδα Συνεργασίας, με τη βοήθεια της Επιτροπής και του ENISA και, κατά περίπτωση, του δικτύου CSIRT καθορίζει, έως τις 17 Ιανουαρίου 2025, τη μεθοδολογία και τις οργανωτικές πτυχές των αξιολογήσεων από ομοτίμους με σκοπό την άντληση διδαγμάτων από κοινές εμπειρίες, την ενίσχυση της αμοιβαίας εμπιστοσύνης, την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, καθώς και την ενίσχυση των ικανοτήτων και των πολιτικών κυβερνοασφάλειας των κρατών μελών που είναι αναγκαίες για την εφαρμογή της παρούσας οδηγίας. Η συμμετοχή σε αξιολογήσεις από ομοτίμους είναι προαιρετική. Οι αξιολογήσεις από ομοτίμους διενεργούνται από εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας. Οι εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας ορίζονται από τουλάχιστον δύο κράτη μέλη, διαφορετικά από το κράτος μέλος που εξετάζεται.

Οι αξιολογήσεις από ομοτίμους καλύπτουν τουλάχιστον ένα από τα ακόλουθα:

α) το επίπεδο εφαρμογής των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και των υποχρεώσεων υποβολής εκθέσεων που προβλέπονται στα άρθρα 21 και 23·

β) το επίπεδο των ικανοτήτων, συμπεριλαμβανομένων των διαθέσιμων οικονομικών, τεχνικών και ανθρώπινων πόρων, και την αποτελεσματικότητα της άσκησης των καθηκόντων εκ μέρους των αρμόδιων αρχών·

γ) τις επιχειρησιακές ικανότητες των CSIRT·

δ) το επίπεδο υλοποίησης της αμοιβαίας συνδρομής που αναφέρεται στο άρθρο 37·

ε) το επίπεδο υλοποίησης των ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρεται στο άρθρο 29·

στ) ειδικά ζητήματα διασυνοριακού ή διατομεακού χαρακτήρα.

2. Η μεθοδολογία που αναφέρεται στην παράγραφο 1 περιλαμβάνει αντικειμενικά, αμερόληπτα, δίκαια και διαφανή κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας προς επιλογή για τη διενέργεια των αξιολογήσεων από ομοτίμους. Η Επιτροπή και ο ENISA συμμετέχουν ως παρατηρητές στις αξιολογήσεις από ομοτίμους.

3. Τα κράτη μέλη μπορούν να προσδιορίσουν συγκεκριμένα ζητήματα όπως αναφέρεται στην παράγραφο 1 στοιχείο στ) για τους σκοπούς της αξιολόγησης από ομοτίμους.

4. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, όπως αναφέρεται στην παράγραφο 1, τα κράτη μέλη κοινοποιούν στα συμμετέχοντα κράτη μέλη το πεδίο εφαρμογής της, μεταξύ άλλων και τα συγκεκριμένα ζητήματα που προσδιορίζονται βάσει της παραγράφου 3.

5. Πριν από την έναρξη της αξιολόγησης από ομοτίμους, τα κράτη μέλη μπορούν να διενεργούν αυτοαξιολόγηση των αξιολογούμενων πτυχών και να παρέχουν την εν λόγω αυτοαξιολόγηση στους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας. Η Ομάδα Συνεργασίας, με τη συνδρομή της Επιτροπής και του ENISA, καθορίζει τη μεθοδολογία για την αυτοαξιολόγηση των κρατών μελών.

6. Οι αξιολογήσεις από ομοτίμους περιλαμβάνουν φυσικές ή εικονικές επιτόπιες επισκέψεις και ανταλλαγές πληροφοριών εκτός των εγκαταστάσεων. Με γνώμονα την αρχή της καλής συνεργασίας, τα κράτη μέλη που υποβάλλονται σε αξιολόγηση από ομοτίμους παρέχουν στους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση, με την επιφύλαξη του ενωσιακού ή του εθνικού δικαίου σχετικά με την προστασία εμπιστευτικών ή διαβαθμισμένων πληροφοριών και τη διασφάλιση ουσιωδών λειτουργιών του κράτους, όπως η εθνική ασφάλεια. Η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, καταρτίζει κατάλληλους κώδικες δεοντολογίας στους οποίους στηρίζονται οι μέθοδοι εργασίας των ορισθέντων εμπειρογνωμόνων κυβερνοασφάλειας. Κάθε πληροφορία που λαμβάνεται μέσω της αξιολόγησης από ομοτίμους χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό. Οι εμπειρογνώμονες κυβερνοασφάλειας που συμμετέχουν στην αξιολόγηση από ομοτίμους δεν αποκαλύπτουν σε τρίτους τυχόν ευαίσθητες ή εμπιστευτικές πληροφορίες που απέκτησαν κατά τη διάρκεια της εν λόγω αξιολόγησης από ομοτίμους.

7. Αφού υποβληθούν σε αξιολόγηση από ομοτίμους, τα σημεία που εξετάζονται σε ένα κράτος μέλος δεν υποβάλλονται σε περαιτέρω αξιολόγηση από ομοτίμους εντός του εν λόγω κράτους μέλους για διάστημα δύο ετών μετά την ολοκλήρωση της αξιολόγησης από ομοτίμους, εκτός εάν αποφασιστεί διαφορετικά από το κράτος μέλος ή συμφωνηθεί μετά από πρόταση της ομάδας συνεργασίας.

8. Τα κράτη μέλη μεριμνούν για τη γνωστοποίηση οποιουδήποτε κινδύνου σύγκρουσης συμφερόντων που αφορά τους ορισθέντες εμπειρογνώμονες κυβερνοασφάλειας στα άλλα κράτη μέλη, στην Ομάδα Συνεργασίας, στην Επιτροπή και στον ENISA, πριν από την έναρξη της αξιολόγησης από ομοτίμους. Το κράτος μέλος που υπόκειται στην αξιολόγηση από ομοτίμους μπορεί να αντιταχθεί στον ορισμό συγκεκριμένων εμπειρογνωμόνων για δεόντως αιτιολογημένους λόγους που κοινοποιούνται στο ορίζον κράτος μέλος.

9. Οι εμπειρογνώμονες κυβερνοασφάλειας που συμμετέχουν σε αξιολογήσεις από ομοτίμους συντάσσουν εκθέσεις με τα ευρήματα και τα συμπεράσματα των αξιολογήσεων. Τα υπό αξιολόγηση από ομοτίμους κράτη μέλη μπορούν να υποβάλλουν παρατηρήσεις σχετικά με τα σχέδια εκθέσεων που τα αφορούν και τα σχόλια αυτά επισυνάπτονται στις εκθέσεις. Οι εκθέσεις περιλαμβάνουν συστάσεις που επιτρέπουν τη βελτίωση των πτυχών που καλύπτονται από την αξιολόγηση από ομοτίμους. Οι εκθέσεις υποβάλλονται στην Ομάδα Συνεργασίας και στο δίκτυο CSIRT, κατά περίπτωση. Τα υπό αξιολόγηση από ομοτίμους κράτη μέλη μπορούν να αποφασίσουν να δημοσιοποιήσουν την έκθεσή τους ή μια αναδιατυπωμένη έκδοσή της.

ΚΕΦΑΛΑΙΟ IV

ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΩΝ

Άρθρο 20

Διακυβέρνηση

1. Τα κράτη μέλη διασφαλίζουν ότι η ανώτατη διοίκηση των βασικών και σημαντικών οντοτήτων εγκρίνει τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνουν οι εν λόγω οντότητες προκειμένου να συμμορφώνονται με το άρθρο 21, επιβλέπει την εφαρμογή τους και μπορεί να λογοδοτεί για την εκ μέρους των οντοτήτων παραβίαση των υποχρεώσεων του εν λόγω άρθρου.

Η εφαρμογή της παρούσας παραγράφου δεν θίγει το εθνικό δίκαιο όσον αφορά τους κανόνες περί ευθύνης που ισχύουν για τους δημόσιους οργανισμούς, καθώς και την ευθύνη δημοσίων υπαλλήλων και αιρετών ή διορισμένων αξιωματούχων.

2. Τα κράτη μέλη διασφαλίζουν ότι τα μέλη της ανώτατης διοίκησης των βασικών και σημαντικών οντοτήτων υποχρεούνται να παρακολουθούν εκπαίδευση και να ενθαρρύνουν τις βασικές και σημαντικές οντότητες να προσφέρουν παρόμοια κατάρτιση στους υπαλλήλους τους σε τακτική βάση, προκειμένου να αποκτούν επαρκείς γνώσεις και δεξιότητες που θα τους επιτρέπουν να εντοπίζουν τους κινδύνους και να αξιολογούν τις πρακτικές διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον αντίκτυπό τους στις υπηρεσίες που παρέχει η οντότητα.

Άρθρο 21

Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας

1. Τα κράτη μέλη εξασφαλίζουν ότι οι βασικές και σημαντικές οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι εν λόγω οντότητες για τις δραστηριότητές τους ή για την παροχή των υπηρεσιών τους και για την πρόληψη ή ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες.

Λαμβάνοντας υπόψη τα πλέον σύγχρονα και, κατά περίπτωση, τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, καθώς και το κόστος εφαρμογής, τα μέτρα που αναφέρονται στο πρώτο εδάφιο εξασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο. Κατά την αξιολόγηση της αναλογικότητας των εν λόγω μέτρων, λαμβάνονται δεόντως υπόψη ο βαθμός έκθεσης της οντότητας σε κινδύνους, το μέγεθος της οντότητας και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους.

2. Τα μέτρα που αναφέρονται στην παράγραφο 1 βασίζονται σε ολιστική προσέγγιση του κινδύνου που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά, περιλαμβάνουν δε τουλάχιστον τα ακόλουθα:

α) πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων·

β) χειρισμό περιστατικών·

γ) επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων·

δ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της·

ε) ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών·

στ) πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

ζ) βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια·

η) πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης·

θ) ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων·

ι) χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση.

3. Τα κράτη μέλη διασφαλίζουν ότι, όταν εξετάζουν ποια από τα μέτρα που αναφέρονται στην παράγραφο 2 στοιχείο δ) του παρόντος άρθρου είναι κατάλληλα, οι οντότητες λαμβάνουν υπόψη τις ευπάθειες που χαρακτηρίζουν κάθε άμεσο προμηθευτή και πάροχο υπηρεσιών και τη συνολική ποιότητα των προϊόντων και των πρακτικών κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους. Τα κράτη μέλη διασφαλίζουν επίσης ότι, όταν εξετάζουν ποια από τα μέτρα που αναφέρονται στο εν λόγω στοιχείο είναι κατάλληλα, οι οντότητες υποχρεούνται να λαμβάνουν υπόψη τα αποτελέσματα των συντονισμένων εκτιμήσεων κινδύνου των κρίσιμων αλυσίδων εφοδιασμού που διενεργούνται σύμφωνα με το άρθρο 22 παράγραφος 1.

4. Τα κράτη μέλη διασφαλίζουν ότι μια οντότητα που διαπιστώνει ότι δεν συμμορφώνεται με τα μέτρα που προβλέπονται στην παράγραφο 2 λαμβάνει αμελλητί όλα τα αναγκαία, κατάλληλα και αναλογικά διορθωτικά μέτρα.

5. Έως τις 17 Οκτωβρίου 2024, η Επιτροπή εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων που αναφέρονται στην παράγραφο 2 όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρου δεδομένων, τους παρόχους δικτύων παράδοσης περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης.

Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων, καθώς και των τομεακών απαιτήσεων, κατά περίπτωση, των μέτρων που αναφέρονται στην παράγραφο 2 όσον αφορά βασικές και σημαντικές οντότητες διαφορετικές από εκείνες που αναφέρονται στο πρώτο εδάφιο της παρούσας παραγράφου.

Κατά την κατάρτιση των εκτελεστικών πράξεων που αναφέρονται στο πρώτο και δεύτερο εδάφιο της παρούσας παραγράφου, η Επιτροπή ακολουθεί, στο μέτρο του δυνατού, τα ευρωπαϊκά και διεθνή πρότυπα, καθώς και τις σχετικές τεχνικές προδιαγραφές. Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας και τον ENISA σχετικά με τα σχέδια εκτελεστικών πράξεων σύμφωνα με το άρθρο 14 παράγραφος 4 στοιχείο ε).

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Άρθρο 22

Συντονισμένες σε ενωσιακό επίπεδο εκτιμήσεις κινδύνου για τις κρίσιμες αλυσίδες εφοδιασμού

1. Η Ομάδα Συνεργασίας, σε συνεργασία με την Επιτροπή και τον ENISA, μπορεί να διενεργεί συντονισμένες εκτιμήσεις κινδύνου για την ασφάλεια συγκεκριμένων κρίσιμων υπηρεσιών ΤΠΕ, συστημάτων ΤΠΕ ή αλυσίδων εφοδιασμού προϊόντων ΤΠΕ, λαμβάνοντας υπόψη τεχνικούς και, κατά περίπτωση, μη τεχνικούς παράγοντες κινδύνου.

2. Η Επιτροπή, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας και τον ENISA, και, κατά περίπτωση, τα σχετικά ενδιαφερόμενα μέρη, προσδιορίζει τις συγκεκριμένες κρίσιμες υπηρεσίες ΤΠΕ, τα συστήματα ΤΠΕ ή τα προϊόντα ΤΠΕ που ενδέχεται να υπόκεινται στη συντονισμένη εκτίμηση κινδύνου ασφάλειας που αναφέρεται στην παράγραφο 1.

Άρθρο 23

Υποχρεώσεις αναφοράς περιστατικών

1. Κάθε κράτος μέλος διασφαλίζει ότι οι βασικές και σημαντικές οντότητες κοινοποιούν αμελλητί στην CSIRT του ή, κατά περίπτωση, στην αρμόδια αρχή του σύμφωνα με την παράγραφο 4 κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους, όπως αναφέρεται στην παράγραφο 3 (σημαντικό περιστατικό). Κατά περίπτωση, οι οικείες οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στους αποδέκτες των υπηρεσιών τους σημαντικά περιστατικά που ενδέχεται να επηρεάσουν αρνητικά την παροχή των εν λόγω υπηρεσιών. Κάθε κράτος μέλος διασφαλίζει ότι οι εν λόγω οντότητες αναφέρουν, μεταξύ άλλων, κάθε πληροφορία που επιτρέπει στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή να προσδιορίσει τυχόν διασυνοριακές επιπτώσεις του περιστατικού. Η απλή πράξη κοινοποίησης δεν συνεπάγεται αυξημένη ευθύνη της κοινοποιούσας οντότητας.

Όταν οι οικείες οντότητες κοινοποιούν στην αρμόδια αρχή σημαντικό περιστατικό σύμφωνα με το πρώτο εδάφιο, το κράτος μέλος διασφαλίζει ότι η εν λόγω αρμόδια αρχή διαβιβάζει την κοινοποίηση στην CSIRT με την παραλαβή της.

Σε περίπτωση διασυνοριακού ή διατομεακού σημαντικού περιστατικού, τα κράτη μέλη διασφαλίζουν ότι τα ενιαία σημεία επαφής τους λαμβάνουν εγκαίρως τις σχετικές πληροφορίες που κοινοποιούνται σύμφωνα με την παράγραφο 4.

2. Κατά περίπτωση, τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες κοινοποιούν αμελλητί στους αποδέκτες των υπηρεσιών τους, που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, τυχόν μέτρα ή διορθωτικές ενέργειες που μπορούν να αυτοί να λάβουν για την αντιμετώπιση της συγκεκριμένης απειλής. Κατά περίπτωση, οι οντότητες ενημερώνουν επίσης τους εν λόγω αποδέκτες για τη σημαντική κυβερνοαπειλή.

3. Ένα περιστατικό θεωρείται σημαντικό εάν:

α) έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα·

β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

4. Τα κράτη μέλη διασφαλίζουν ότι, για τους σκοπούς της κοινοποίησης δυνάμει της παραγράφου 1, οι οικείες οντότητες υποβάλλουν στην CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή:

α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που αντιλήφθηκε το σημαντικό περιστατικό, έγκαιρη προειδοποίηση, η οποία, κατά περίπτωση, αναφέρει αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από έκνομες ή κακόβουλες ενέργειες ή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·

β) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, κοινοποίηση περιστατικού, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες που αναφέρονται στο στοιχείο α) και αναφέρει μια αρχική αξιολόγηση του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και, εφόσον υπάρχουν, τις ενδείξεις της παραβίασης·

γ) κατόπιν αιτήματος μιας CSIRT ή, κατά περίπτωση, της αρμόδιας αρχής, ενδιάμεση έκθεση σχετικά με τις σχετικές επικαιροποιήσεις της κατάστασης·

δ) τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της κοινοποίησης περιστατικού σύμφωνα με το στοιχείο β), η οποία περιλαμβάνει τα ακόλουθα:

i) λεπτομερή περιγραφή του περιστατικού, μεταξύ άλλων της σοβαρότητάς του και των επιπτώσεών του·

ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·

iii) εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού·

iv) κατά περίπτωση, τον διασυνοριακό αντίκτυπο του περιστατικού·

ε) σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης που αναφέρεται στο στοιχείο δ), τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι οικείες οντότητες υποβάλλουν έκθεση προόδου τη δεδομένη στιγμή και τελική έκθεση εντός ενός μηνός από τον εκ μέρους τους χειρισμό του σημαντικού περιστατικού.

Κατά παρέκκλιση από το πρώτο εδάφιο στοιχείο β), ο πάροχος υπηρεσιών εμπιστοσύνης ενημερώνει την CSIRT ή, κατά περίπτωση, την αρμόδια αρχή, όσον αφορά σημαντικά περιστατικά που επηρεάζουν την παροχή των υπηρεσιών εμπιστοσύνης του, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έλαβε γνώση του σημαντικού περιστατικού.

5. Η CSIRT ή η αρμόδια αρχή παρέχει στην κοινοποιούσα οντότητα, αμελλητί και ει δυνατόν εντός 24 ωρών από τη λήψη της έγκαιρης προειδοποίησης που αναφέρεται στην παράγραφο 4 στοιχείο α), απάντηση που συμπεριλαμβάνει αρχική ανάδραση σχετικά με το σημαντικό περιστατικό και, κατόπιν αιτήματος της οντότητας, καθοδήγηση ή επιχειρησιακές συμβουλές σχετικά με την εφαρμογή πιθανών μέτρων μετριασμού. Σε περίπτωση που η CSIRT δεν είναι η αρχική αποδέκτρια της κοινοποίησης που αναφέρεται στην παράγραφο 1, η καθοδήγηση παρέχεται από την αρμόδια αρχή σε συνεργασία με την CSIRT. Η CSIRT παρέχει πρόσθετη τεχνική υποστήριξη εφόσον το ζητήσει η οικεία οντότητα. Όταν υπάρχουν υπόνοιες ότι το σημαντικό περιστατικό είναι ποινικού χαρακτήρα, η CSIRT ή η αρμόδια αρχή παρέχει επίσης καθοδήγηση σχετικά με την αναφορά του σημαντικού περιστατικού στις αρχές επιβολής του νόμου.

6. Κατά περίπτωση, και ιδίως όταν το σημαντικό περιστατικό αφορά δύο ή περισσότερα κράτη μέλη, η CSIRT, η αρμόδια αρχή ή το ενιαίο σημείο επαφής ενημερώνουν αμελλητί τα άλλα επηρεαζόμενα κράτη μέλη και τον ENISA σχετικά με το σημαντικό περιστατικό. Οι πληροφορίες αυτές περιλαμβάνουν το είδος των πληροφοριών που λαμβάνονται σύμφωνα με την παράγραφο 4. Στο πλαίσιο αυτό, η CSIRT, η αρμόδια αρχή ή το ενιαίο σημείο επαφής διαφυλάσσουν, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, την ασφάλεια και τα εμπορικά συμφέροντα της οντότητας, καθώς και την εμπιστευτικότητα των παρεχόμενων πληροφοριών.

7. Όταν η ευαισθητοποίηση του κοινού είναι αναγκαία για την πρόληψη σημαντικού περιστατικού ή για την αντιμετώπιση συνεχιζόμενου σημαντικού περιστατικού, ή όταν η γνωστοποίηση του σημαντικού περιστατικού είναι άλλως προς το δημόσιο συμφέρον, η CSIRT ενός κράτους μέλους ή, κατά περίπτωση, η αρμόδια αρχή του και, κατά περίπτωση, οι CSIRT ή οι αρμόδιες αρχές άλλων ενδιαφερόμενων κρατών μελών, μπορούν, κατόπιν διαβούλευσης με την οικεία οντότητα, να ενημερώσουν το κοινό σχετικά με το σημαντικό περιστατικό ή να απαιτήσουν από την οντότητα να το πράξει.

8. Κατόπιν αιτήματος της CSIRT ή της αρμόδιας αρχής, το ενιαίο σημείο επαφής διαβιβάζει τις κοινοποιήσεις που λαμβάνονται σύμφωνα με την παράγραφο 1 στα ενιαία σημεία επαφής άλλων επηρεαζόμενων κρατών μελών.

9. Το ενιαίο σημείο επαφής υποβάλλει στον ENISA ανά τρίμηνο συνοπτική έκθεση, η οποία περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με σημαντικά περιστατικά, περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και με το άρθρο 30. Προκειμένου να συμβάλει στην παροχή συγκρίσιμων πληροφοριών, ο ENISA μπορεί να εκδίδει τεχνικές οδηγίες σχετικά με τις παραμέτρους των πληροφοριών που πρέπει να περιλαμβάνονται στη συνοπτική έκθεση. Ο ENISA ενημερώνει την Ομάδα Συνεργασίας και το δίκτυο CSIRT σχετικά με τα πορίσματά του σχετικά με τις κοινοποιήσεις που λαμβάνει κάθε έξι μήνες.

10. Οι CSIRT ή, κατά περίπτωση, οι αρμόδιες αρχές παρέχουν στις αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 πληροφορίες σχετικά με σημαντικά περιστατικά, περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και το άρθρο 30 από οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της οδηγίας (ΕΕ) 2022/2557.

11. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό του είδους των πληροφοριών, του μορφότυπου και της διαδικασίας κοινοποίησης που υποβάλλεται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και το άρθρο 30, καθώς και της κοινοποίησης που υποβάλλεται σύμφωνα με την παράγραφο 2 του παρόντος άρθρου.

Έως τις 17 Οκτωβρίου 2024, η Επιτροπή εκδίδει, όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, καθώς και τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό, όπως αναφέρεται στην παράγραφο 3. Η Επιτροπή μπορεί να εκδίδει τέτοιες εκτελεστικές πράξεις όσον αφορά άλλες βασικές και σημαντικές οντότητες.

Η Επιτροπή ανταλλάσσει συμβουλές και συνεργάζεται με την Ομάδα Συνεργασίας και τον ENISA σχετικά με τα σχέδια εκτελεστικών πράξεων σύμφωνα με το άρθρο 14 παράγραφος 4 στοιχείο ε).

Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 39 παράγραφος 2.

Άρθρο 24

Χρήση των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Προκειμένου να αποδειχθεί η συμμόρφωση με τις ειδικές απαιτήσεις του άρθρου 21, τα κράτη μέλη μπορούν να απαιτούν από βασικές και σημαντικές οντότητες να χρησιμοποιούν συγκεκριμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, που αναπτύσσονται από τη βασική ή σημαντική οντότητα ή παρέχονται από τρίτους και πιστοποιούνται στο πλαίσιο ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας που θεσπίζονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Επιπλέον, τα κράτη μέλη ενθαρρύνουν τις βασικές και σημαντικές οντότητες να χρησιμοποιούν αναγνωρισμένες υπηρεσίες εμπιστοσύνης.

2. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 38, για να συμπληρώνει την παρούσα οδηγία προσδιορίζοντας τις κατηγορίες βασικών και σημαντικών οντοτήτων από τις οποίες θα απαιτείται να χρησιμοποιούν ορισμένα πιστοποιημένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ ή να λαμβάνουν πιστοποιητικό δυνάμει ευρωπαϊκού συστήματος πιστοποίησης κυβερνοασφάλειας εγκεκριμένου σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Οι εν λόγω κατ' εξουσιοδότηση πράξεις εκδίδονται όταν έχουν εντοπιστεί ανεπαρκή επίπεδα κυβερνοασφάλειας, και περιλαμβάνουν περίοδο εφαρμογής.

Πριν από την έκδοση των εν λόγω κατ' εξουσιοδότηση πράξεων, η Επιτροπή διενεργεί εκτίμηση επιπτώσεων και διενεργεί διαβουλεύσεις σύμφωνα με το άρθρο 56 του κανονισμού (ΕΕ) 2019/881.

3. Όταν δεν είναι διαθέσιμο κατάλληλο ευρωπαϊκό σύστημα πιστοποίησης κυβερνοασφάλειας για τους σκοπούς της παραγράφου 2 του παρόντος άρθρου, η Επιτροπή μπορεί, κατόπιν διαβούλευσης με την Ομάδα Συνεργασίας και την Ευρωπαϊκή Ομάδα Πιστοποίησης Κυβερνοασφάλειας, να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα σύμφωνα με το άρθρο 48 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881.

Άρθρο 25

Τυποποίηση

1. Προκειμένου να προωθηθεί η συγκλίνουσα εφαρμογή του άρθρου 21 παράγραφοι 1 και 2, τα κράτη μέλη, χωρίς να επιβάλλουν ούτε να ευνοούν τη χρήση συγκεκριμένου είδους τεχνολογίας, ενθαρρύνουν τη χρήση ευρωπαϊκών και διεθνώς αποδεκτών προτύπων και τεχνικών προδιαγραφών σχετικών με την ασφάλεια συστημάτων δικτύου και πληροφοριών.

2. Ο ENISA, σε συνεργασία με τα κράτη μέλη και, κατά περίπτωση, κατόπιν διαβούλευσης με τα ενδιαφερόμενα μέρη, καταρτίζει συμβουλές και κατευθυντήριες γραμμές σχετικά με τους τεχνικούς τομείς που πρέπει να εξεταστούν σε σχέση με την παράγραφο 1, καθώς και σχετικά με τα ήδη υφιστάμενα πρότυπα, συμπεριλαμβανομένων των εθνικών προτύπων, που θα επιτρέψουν την κάλυψη των εν λόγω τομέων.

ΚΕΦΑΛΑΙΟ V

ΔΙΚΑΙΟΔΟΣΙΑ ΚΑΙ ΚΑΤΑΧΩΡΙΣΗ

Άρθρο 26

Δικαιοδοσία και εδαφικότητα

1. Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θεωρούνται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένες, εκτός αν πρόκειται για:

α) παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οι οποίοι θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους·

β) παρόχους υπηρεσιών DNS, μητρώα ονομάτων TLD, οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχους υπηρεσιών υπολογιστικού νέφους, παρόχους υπηρεσιών κέντρων δεδομένων, παρόχους δικτύων διανομής περιεχομένου, παρόχους διαχειριζομένων υπηρεσιών, παρόχους διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, που θεωρείται ότι εμπίπτουν στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση σύμφωνα με την παράγραφο 2·

γ) οντότητες δημόσιας διοίκησης, που θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους που τις έχει συστήσει.

2. Για τους σκοπούς της παρούσας οδηγίας, οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) θεωρείται ότι έχει την κύρια εγκατάστασή της στην Ένωση στο κράτος μέλος στο οποίο λαμβάνονται κυρίως οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί ή εάν οι αποφάσεις αυτές δεν λαμβάνονται στην Ένωση, η κύρια εγκατάσταση θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο διεξάγονται οι επιχειρήσεις κυβερνοασφάλειας. Εάν το εν λόγω κράτος μέλος δεν μπορεί να προσδιοριστεί, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο η οικεία οντότητα έχει την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση.

3. Εάν μια οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) δεν είναι εγκατεστημένη στην Ένωση, αλλά προσφέρει υπηρεσίες εντός της Ένωσης, ορίζει εκπρόσωπο στην Ένωση. Ο εκπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη μέλη στα οποία προσφέρονται οι υπηρεσίες. Μια τέτοια οντότητα θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκπρόσωπος. Ελλείψει εκπροσώπου στην Ένωση που ορίζεται σύμφωνα με την παρούσα παράγραφο, κάθε κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες μπορεί να κινήσει νομικές διαδικασίες κατά της οντότητας για παραβίαση των υποχρεώσεων της παρούσας οδηγίας.

4. Ο ορισμός εκπροσώπου από οντότητα που αναφέρεται στην παράγραφο 1 στοιχείο β) δεν θίγει τις νομικές ενέργειες που θα μπορούσαν να κινηθούν κατά της ίδιας της οντότητας.

5. Τα κράτη μέλη που έχουν λάβει αίτημα αμοιβαίας συνδρομής σε σχέση με οντότητα που αναφέρεται στην παράγραφο 1, μπορούν, εντός των ορίων του εν λόγω αιτήματος, να λαμβάνουν κατάλληλα μέτρα εποπτείας και επιβολής σε σχέση με την οικεία οντότητα η οποία παρέχει υπηρεσίες ή διαθέτει το σύστημα δικτύου και πληροφοριών στην επικράτειά τους.

Άρθρο 27

Μητρώο οντοτήτων

1. Ο ENISA δημιουργεί και τηρεί μητρώο με παρόχους υπηρεσιών DNS, μητρώα ονομάτων TLD, οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα, παρόχους υπηρεσιών υπολογιστικού νέφους, παρόχους υπηρεσιών κέντρων δεδομένων, παρόχους δικτύων διανομής περιεχομένου, παρόχους διαχειριζομένων υπηρεσιών, παρόχους διαχειριζομένων υπηρεσιών ασφάλειας, καθώς και παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης ή πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, βάσει των πληροφοριών που λαμβάνει από τα ενιαία σημεία επαφής σύμφωνα με την παράγραφο 4. Κατόπιν αιτήματος, ο ENISA επιτρέπει την πρόσβαση των αρμόδιων αρχών στο εν λόγω μητρώο, διασφαλίζοντας παράλληλα την προστασία της εμπιστευτικότητας των πληροφοριών, κατά περίπτωση.

2. Τα κράτη μέλη απαιτούν από τις οντότητες που αναφέρονται στην παράγραφο 1 να υποβάλουν τις ακόλουθες πληροφορίες στις αρμόδιες αρχές έως τις 17 Ιανουαρίου 2025:

α) την επωνυμία της οντότητας·

β) τον σχετικό τομέα, υποτομέα και τύπο οντότητας που αναφέρεται στα παραρτήματα I και II, κατά περίπτωση·

γ) τη διεύθυνση της κύριας εγκατάστασης της οντότητας και των άλλων νομικών εγκαταστάσεών της στην Ένωση ή, εάν δεν είναι εγκατεστημένη στην Ένωση, της διεύθυνσης του εκπροσώπου της που έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφος 3·

δ) επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των αριθμών τηλεφώνου της οντότητας και, κατά περίπτωση, του εκπροσώπου της ο οποίος έχει οριστεί σύμφωνα με το άρθρο 26 παράγραφος 3·

ε) τα κράτη μέλη στα οποία η οντότητα παρέχει υπηρεσίες· και

στ) το εύρος IP της οντότητας.

3. Τα κράτη μέλη διασφαλίζουν ότι οι οντότητες που αναφέρονται στην παράγραφο 1 κοινοποιούν στην αρμόδια αρχή τυχόν αλλαγές στις πληροφορίες που υπέβαλαν δυνάμει της παραγράφου 2 αμελλητί και, σε κάθε περίπτωση, εντός τριών μηνών από την ημερομηνία πραγματοποίησης της αλλαγής.

4. Με την παραλαβή των πληροφοριών που αναφέρονται στις παραγράφους 2 και 3, εκτός από τις πληροφορίες που αναφέρονται στην παράγραφο 2 στοιχείο στ), το ενιαίο σημείο επαφής του οικείου κράτους μέλους τις διαβιβάζει), στον ENISA χωρίς αδικαιολόγητη καθυστέρηση.

5. Κατά περίπτωση, οι πληροφορίες που αναφέρονται στις παραγράφους 2 και 3 του παρόντος άρθρου υποβάλλονται μέσω του εθνικού μηχανισμού που αναφέρεται στο άρθρο 3 παράγραφος 4 τέταρτο εδάφιο.

Άρθρο 28

Βάση δεδομένων καταχώρισης ονομάτων τομέα

1. Για τους σκοπούς της συμβολής στην ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του DNS, τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να συλλέγουν και να διατηρούν ακριβή και πλήρη δεδομένα καταχώρισης ονομάτων τομέα σε ειδική βάση δεδομένων με τη δέουσα επιμέλεια σύμφωνα με την ενωσιακή νομοθεσία για την προστασία των δεδομένων όσον αφορά τα δεδομένα προσωπικού χαρακτήρα.

2. Για τους σκοπούς της παραγράφου 1, τα κράτη μέλη απαιτούν η βάση δεδομένων καταχώρισης ονομάτων τομέα να περιέχει τις αναγκαίες πληροφορίες για την ταυτοποίηση και την επικοινωνία με τους κατόχους των ονομάτων τομέα και τα σημεία επαφής που διαχειρίζονται τα ονόματα τομέα στο πλαίσιο των TLD. Οι πληροφορίες αυτές περιλαμβάνουν:

α) το όνομα τομέα·

β) την ημερομηνία καταχώρισης·

γ) το όνομα, την ηλεκτρονική διεύθυνση επικοινωνίας και τον αριθμό τηλεφώνου του καταχωρίζοντος·

δ) τη διεύθυνση ηλεκτρονικού ταχυδρομείου επικοινωνίας και τον αριθμό τηλεφώνου του σημείου επαφής που διαχειρίζεται το όνομα τομέα σε περίπτωση που διαφέρουν από εκείνα του καταχωρίζοντος.

3. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να διαθέτουν πολιτικές και διαδικασίες, συμπεριλαμβανομένων διαδικασιών επαλήθευσης, ώστε να διασφαλίζεται ότι οι βάσεις δεδομένων που αναφέρονται στην παράγραφο 1 περιλαμβάνουν ακριβείς και πλήρεις πληροφορίες. Τα κράτη μέλη απαιτούν να δημοσιοποιούνται οι εν λόγω πολιτικές και διαδικασίες.

4. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και από τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να δημοσιοποιούν αμελλητί μετά από την καταχώριση ονόματος τομέα, τα δεδομένα καταχώρισης ονομάτων τομέα που δεν είναι δεδομένα προσωπικού χαρακτήρα.

5. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να παρέχουν πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα κατόπιν νομίμων και δεόντως αιτιολογημένων αιτημάτων από νόμιμους αιτούντες πρόσβαση, σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να απαντούν χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από την παραλαβή τυχόν αιτημάτων πρόσβασης. Τα κράτη μέλη απαιτούν να δημοσιοποιούνται οι πολιτικές και οι διαδικασίες γνωστοποίησης των εν λόγω δεδομένων.

6. Η συμμόρφωση με τις υποχρεώσεις που ορίζονται στις παραγράφους 1 έως 5 δεν οδηγεί σε επικάλυψη της συλλογής δεδομένων καταχώρισης ονομάτων τομέα. Για τον σκοπό αυτό, τα κράτη μέλη απαιτούν από τα μητρώα ονομάτων TLD και τις οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα να συνεργάζονται μεταξύ τους.

ΚΕΦΑΛΑΙΟ VI

ΑΝΤΑΛΛΑΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 29

Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας

1. Τα κράτη μέλη διασφαλίζουν ότι οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας και, κατά περίπτωση, άλλες οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας είναι σε θέση να ανταλλάσσουν μεταξύ τους, σε εθελοντική βάση, πληροφορίες σχετικές με την κυβερνοασφάλεια, συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, ευπάθειες, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

α) αποσκοπεί στην πρόληψη, τον εντοπισμό, την αντιμετώπιση ή την ανάκαμψη από περιστατικά ή στον μετριασμό των επιπτώσεών τους·

β) ενισχύει το επίπεδο της κυβερνοασφάλειας, ιδίως μέσω της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των εν λόγω απειλών, της στήριξης μιας σειράς αμυντικών ικανοτήτων, της αποκατάστασης και της γνωστοποίησης ευπαθειών, της ανίχνευσης απειλών, των τεχνικών περιορισμού και πρόληψης, των στρατηγικών μετριασμού ή των σταδίων αντίδρασης και ανάκαμψης ή της προώθησης της συνεργατικής έρευνας για τις κυβερνοαπειλές μεταξύ δημόσιων και ιδιωτικών φορέων.

2. Τα κράτη μέλη διασφαλίζουν ότι η ανταλλαγή πληροφοριών πραγματοποιείται στο πλαίσιο κοινοτήτων βασικών και σημαντικών οντοτήτων και, κατά περίπτωση, των προμηθευτών ή των παρόχων υπηρεσιών τους. Η εν λόγω ανταλλαγή πραγματοποιείται μέσω ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας όσον αφορά τον δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών.

3. Τα κράτη μέλη διευκολύνουν τη θέσπιση ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2 του παρόντος άρθρου. Οι ρυθμίσεις αυτές μπορούν να προσδιορίζουν επιχειρησιακά στοιχεία, συμπεριλαμβανομένων της χρήσης ειδικών πλατφορμών ΤΠΕ και εργαλείων αυτοματισμού, του περιεχομένου και των όρων των ρυθμίσεων ανταλλαγής πληροφοριών. Κατά τον καθορισμό των λεπτομερειών της συμμετοχής των δημόσιων αρχών στις εν λόγω ρυθμίσεις, τα κράτη μέλη μπορούν να επιβάλλουν όρους όσον αφορά τις πληροφορίες που διατίθενται από τις αρμόδιες αρχές ή τις CSIRT. Τα κράτη μέλη παρέχουν βοήθεια για την εφαρμογή των εν λόγω ρυθμίσεων σύμφωνα με τις πολιτικές τους που αναφέρονται στο άρθρο 7 παράγραφος 2 στοιχείο η).

4. Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες γνωστοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, αμέσως μετά τη σύναψη των εν λόγω ρυθμίσεων ή, κατά περίπτωση, την ανάκληση της συμμετοχής τους στις ρυθμίσεις αυτές, μόλις αυτή πραγματοποιηθεί.

5. Ο ENISA παρέχει συνδρομή για τη θέσπιση ρυθμίσεων ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, ανταλλάσσοντας βέλτιστες πρακτικές και παρέχοντας καθοδήγηση.

Άρθρο 30

Εθελούσια κοινοποίηση των σχετικών πληροφοριών

1. Τα κράτη μέλη διασφαλίζουν ότι, επιπλέον της υποχρέωσης κοινοποίησης που προβλέπεται στο άρθρο 23, οι κοινοποιήσεις μπορούν να υποβάλλονται στις CSIRT ή, κατά περίπτωση, στις αρμόδιες αρχές, σε εθελοντική βάση, από:

α) βασικές και σημαντικές οντότητες όσον αφορά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά·

β) οντότητες διαφορετικές από εκείνες που αναφέρονται στο στοιχείο α), ανεξαρτήτως του αν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, όσον αφορά σημαντικά περιστατικά, κυβερνοαπειλές και παρ' ολίγον περιστατικά.

2. Τα κράτη μέλη επεξεργάζονται τις κοινοποιήσεις που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου με τη διαδικασία του άρθρου 23. Τα κράτη μέλη μπορούν να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων.

Όπου είναι αναγκαίο, οι CSIRT και, κατά περίπτωση, οι αρμόδιες αρχές παρέχουν στα ενιαία σημεία επαφής τις πληροφορίες σχετικά με τις κοινοποιήσεις που λαμβάνουν σύμφωνα με το παρόν άρθρο, διασφαλίζοντας παράλληλα την εμπιστευτικότητα και την κατάλληλη προστασία των πληροφοριών που παρέχονται από την αναφέρουσα οντότητα. Με την επιφύλαξη της πρόληψης, της διερεύνησης, της διακρίβωσης και της δίωξης ποινικών αδικημάτων, η εθελούσια αναφορά δεν συνεπάγεται την επιβολή πρόσθετων υποχρεώσεων στην κοινοποιούσα οντότητα, τις οποίες δεν θα υπείχε αν δεν είχε υποβάλει την κοινοποίηση.

ΚΕΦΑΛΑΙΟ VII

ΕΠΟΠΤΕΙΑ ΚΑΙ ΕΠΙΒΟΛΗ

Άρθρο 31

Γενικές πτυχές που αφορούν την εποπτεία και την επιβολή

1. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους εποπτεύουν αποτελεσματικά και λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν τη συμμόρφωση με την παρούσα οδηγία.

2. Τα κράτη μέλη μπορούν να επιτρέπουν στις αρμόδιες αρχές τους να δίνουν προτεραιότητα στα εποπτικά καθήκοντα. Η προτεραιοποίηση αυτή βασίζεται σε προσέγγιση βάσει κινδύνου. Για τον σκοπό αυτό, κατά την άσκηση των εποπτικών καθηκόντων τους που προβλέπονται στα άρθρα 32 και 33, οι αρμόδιες αρχές μπορούν να θεσπίζουν μεθοδολογίες εποπτείας που επιτρέπουν την ιεράρχηση των εν λόγω καθηκόντων με μια προσέγγιση βάσει κινδύνου.

3. Οι αρμόδιες αρχές συνεργάζονται στενά με τις εποπτικές αρχές δυνάμει του κανονισμού (ΕΕ) 2016/679 στην αντιμετώπιση περιστατικών που οδηγούν σε παραβιάσεις δεδομένων προσωπικού χαρακτήρα, με την επιφύλαξη της αρμοδιότητας και των καθηκόντων των εποπτικών αρχών δυνάμει του εν λόγω κανονισμού.

4. Με την επιφύλαξη των εθνικών νομοθετικών και θεσμικών πλαισίων, τα κράτη μέλη διασφαλίζουν ότι, κατά την εποπτεία της συμμόρφωσης των φορέων δημόσιας διοίκησης με την παρούσα οδηγία και την πρόβλεψη μέτρων επιβολής για παραβιάσεις της παρούσας οδηγίας, οι αρμόδιες αρχές διαθέτουν κατάλληλες εξουσίες για την εκτέλεση των καθηκόντων αυτών με λειτουργική ανεξαρτησία έναντι των εποπτευόμενων φορέων δημόσιας διοίκησης. Τα κράτη μέλη μπορούν να αποφασίσουν την επιβολή κατάλληλων, αναλογικών και αποτελεσματικών μέτρων εποπτείας και επιβολής σε σχέση με τις εν λόγω οντότητες σύμφωνα με το εθνικό νομοθετικό και θεσμικό πλαίσιο.

Άρθρο 32

Μέτρα εποπτείας και επιβολής σε σχέση με βασικές οντότητες

1. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα εποπτείας ή επιβολής που επιβάλλονται σε βασικές οντότητες σε σχέση με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών τους καθηκόντων σε σχέση με βασικές οντότητες, έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες σε διαδικασίες που αφορούν τουλάχιστον:

α) επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων, που διεξάγονται από καταρτισμένους επαγγελματίες·

β) τακτικούς και στοχευμένους ελέγχους ασφάλειας που διενεργούνται από ειδικευμένο ανεξάρτητο όργανο ή αρμόδια αρχή·

γ) έκτακτους ειδικούς ελέγχους, μεταξύ άλλων, όταν αυτό δικαιολογείται λόγω σημαντικού περιστατικού ή παραβίασης της παρούσας οδηγίας από τη βασική οντότητα·

δ) σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου, όπου απαιτείται με τη συνεργασία της οικείας οντότητας·

ε) αιτήματα παροχής πληροφοριών αναγκαίων για την εκ των υστέρων αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και της συμμόρφωσης με την υποχρέωση διαβίβασης πληροφοριών στις αρμόδιες αρχές σύμφωνα με το άρθρο 27·

στ) αιτήματα πρόσβασης σε δεδομένα, έγγραφα και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων τους·

ζ) αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

Οι στοχευμένοι έλεγχοι ασφάλειας που αναφέρονται στο πρώτο εδάφιο στοιχείο β) βασίζονται σε εκτιμήσεις κινδύνου που διενεργούνται από την αρμόδια αρχή ή την ελεγχόμενη οντότητα ή σε άλλες σχετικές με κινδύνους διαθέσιμες πληροφορίες.

Τα αποτελέσματα κάθε στοχευμένου ελέγχου ασφάλειας τίθενται στη διάθεση της αρμόδιας αρχής. Το κόστος του εν λόγω στοχευμένου ελέγχου ασφάλειας που διενεργείται από ανεξάρτητο όργανο καλύπτεται από την ελεγχόμενη οντότητα, εκτός από δεόντως αιτιολογημένες περιπτώσεις για τις οποίες η αρμόδια αρχή αποφασίζει διαφορετικά.

3. Κατά την άσκηση των εξουσιών τους σύμφωνα με την παράγραφο 2 στοιχείο ε), στ) ή ζ), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους, κατά την άσκηση των εποπτικών καθηκόντων τους σε σχέση με βασικές οντότητες, έχουν την εξουσία τουλάχιστον για τα ακόλουθα:

α) να εκδίδουν προειδοποιήσεις σχετικά με παραβιάσεις της παρούσας οδηγίας από τις οικείες οντότητες·

β) να εκδίδουν δεσμευτικές οδηγίες, μεταξύ άλλων όσον αφορά τα μέτρα που είναι αναγκαία για την πρόληψη ή την αποκατάσταση περιστατικού, καθώς και προθεσμίες για την εφαρμογή των εν λόγω μέτρων και για την υποβολή εκθέσεων σχετικά με την εφαρμογή τους, ή εντολή με την οποία ζητείται από τις οικείες οντότητες να αποκαταστήσουν τις ελλείψεις που εντοπίστηκαν ή τις παραβιάσεις της παρούσας οδηγίας·

γ) να εντέλλουν τις οικείες οντότητες να παύσουν συμπεριφορά που παραβιάζει την παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·

δ) να εντέλλουν τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας συμμορφώνονται με το άρθρο 21 ή να εκπληρώσουν τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο άρθρο 23, με συγκεκριμένο τρόπο και εντός καθορισμένου χρονικού διαστήματος·

ε) να εντέλλουν τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα σε σχέση με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής·

στ) να δίνουν εντολή στις οικείες οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν ως αποτέλεσμα ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να ορίζουν υπεύθυνο παρακολούθησης με σαφώς καθορισμένα καθήκοντα για καθορισμένο χρονικό διάστημα, προκειμένου να επιβλέπει τη συμμόρφωση των οικείων οντοτήτων με τα άρθρα 21 και 23·

η) να εντέλλουν τις οικείες οντότητες να δημοσιοποιούν πτυχές των παραβιάσεων της παρούσας οδηγία με συγκεκριμένο τρόπο·

θ) να επιβάλλουν, ή να απαιτούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, διοικητικού προστίμου δυνάμει του άρθρου 34 επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στα στοιχεία α) έως η) της παρούσας παραγράφου.

5. Όταν τα μέτρα επιβολής που θεσπίζονται σύμφωνα με την παράγραφο 4 στοιχεία α) έως δ) και στ) είναι αναποτελεσματικά, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους έχουν την εξουσία να ορίζουν προθεσμία εντός της οποίας η βασική οντότητα καλείται να λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή για τη συμμόρφωση με τις απαιτήσεις των εν λόγω αρχών. Εάν τα ζητούμενα μέτρα δεν ληφθούν εντός της καθορισμένης προθεσμίας, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία:

α) να αναστείλουν προσωρινά ή να ζητήσουν από φορέα πιστοποίησης ή εξουσιοδότησης, ή από δικαστήριο, σύμφωνα με το εθνικό δίκαιο, την προσωρινή αναστολή πιστοποίησης ή εξουσιοδότησης που αφορά μέρος ή το σύνολο των σχετικών υπηρεσιών που παρέχονται ή των δραστηριοτήτων που εκτελούνται από τη βασική οντότητα·

β) να ζητούν από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, να απαγορεύουν προσωρινά σε κάθε φυσικό πρόσωπο που είναι υπεύθυνο για την άσκηση διευθυντικών καθηκόντων σε επίπεδο διευθύνοντος συμβούλου ή νομικού εκπροσώπου στη βασική οντότητα να ασκεί διευθυντικά καθήκοντα στην εν λόγω οντότητα.

Οι προσωρινές αναστολές ή απαγορεύσεις που επιβάλλονται σύμφωνα με την παρούσα παράγραφο εφαρμόζονται μόνο έως ότου η οικεία οντότητα λάβει τα αναγκαία μέτρα για να διορθώσει τις ελλείψεις ή να συμμορφωθεί με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες εφαρμόστηκαν τέτοια μέτρα επιβολής. Η επιβολή τέτοιων προσωρινών αναστολών ή απαγορεύσεων υπόκειται σε κατάλληλες διαδικαστικές εγγυήσεις σύμφωνα με τις γενικές αρχές του δικαίου της Ένωσης και του Χάρτη, συμπεριλαμβανομένου του δικαιώματος αποτελεσματικής δικαστικής προστασίας και δίκαιης δίκης, του τεκμηρίου αθωότητας και των δικαιωμάτων υπεράσπισης.

Τα μέτρα επιβολής που προβλέπονται στην παρούσα παράγραφο δεν εφαρμόζονται σε φορείς δημόσιας διοίκησης που υπόκεινται στην παρούσα οδηγία.

6. Τα κράτη μέλη διασφαλίζουν ότι κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως νόμιμος εκπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει την εξουσία να διασφαλίζει τη συμμόρφωσή της με την παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των υποχρεώσεών τους, ώστε να εξασφαλίζεται η συμμόρφωση με την παρούσα οδηγία.

Η εφαρμογή της παρούσας παραγράφου δεν θίγει το εθνικό δίκαιο όσον αφορά τους κανόνες περί ευθύνης που ισχύουν για τους δημόσιους οργανισμούς, καθώς και την ευθύνη δημοσίων υπαλλήλων και αιρετών ή διορισμένων αξιωματούχων.

7. Όταν λαμβάνουν οποιοδήποτε από τα μέτρα επιβολής που αναφέρονται στην παράγραφο 4 ή 5, οι αρμόδιες αρχές σέβονται τα δικαιώματα υπεράσπισης και λαμβάνουν υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης και, τουλάχιστον, λαμβάνουν δεόντως υπόψη:

α) τη σοβαρότητα της παράβασης και τη σημασία των διατάξεων που παραβιάζονται, ενώ τα ακόλουθα, μεταξύ άλλων, θεωρούνται σοβαρές παραβάσεις σε κάθε περίπτωση:

i) οι επανειλημμένες παραβάσεις·

ii) η μη κοινοποίηση ή αποκατάσταση σημαντικών περιστατικών·

iii) η μη αποκατάσταση ελλείψεων σύμφωνα με δεσμευτικές οδηγίες των αρμόδιων αρχών·

iv) η παρεμπόδιση των ελέγχων ή των δραστηριοτήτων παρακολούθησης που διατάσσονται από την αρμόδια αρχή μετά τη διαπίστωση παράβασης·

v) η παροχή ψευδών ή κατάφωρα ανακριβών πληροφοριών σε σχέση με τα μέτρα διαχείρισης κινδύνου ή τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στα άρθρα 21 και 23·

β) τη διάρκεια της παράβασης·

γ) τυχόν σχετικές προηγούμενες παραβάσεις από την οικεία οντότητα·

δ) οποιαδήποτε υλική ή μη υλική ζημία που προκλήθηκε, συμπεριλαμβανομένης της χρηματοοικονομικής ή οικονομικής ζημίας, τις επιπτώσεις σε άλλες υπηρεσίες και τον αριθμό των θιγόμενων χρηστών·

ε) οποιαδήποτε πρόθεση ή αμέλεια εκ μέρους του δράστη της παράβασης·

στ) οποιαδήποτε μέτρα που λαμβάνει η οντότητα για την πρόληψη ή τον μετριασμό της υλικής ή μη υλικής ζημίας·

ζ) οποιαδήποτε τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης·

η) τον βαθμό συνεργασίας των υπαίτιων φυσικών ή νομικών προσώπων με τις αρμόδιες αρχές.

8. Οι αρμόδιες αρχές αιτιολογούν λεπτομερώς τα μέτρα επιβολής τους. Πριν από τη λήψη των μέτρων αυτών, οι αρμόδιες αρχές κοινοποιούν στις ενδιαφερόμενες οντότητες τα προκαταρκτικά πορίσματά τους. Παρέχουν επίσης εύλογο χρονικό διάστημα στις οικείες οντότητες για να υποβάλουν παρατηρήσεις, εκτός από δεόντως αιτιολογημένες περιπτώσεις όπου διαφορετικά θα παρεμποδιζόταν η ανάληψη άμεσης δράσης για την πρόληψη ή την αντιμετώπιση περιστατικών.

9. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν τις σχετικές αρμόδιες αρχές εντός του ίδιου κράτους μέλους δυνάμει της οδηγίας (ΕΕ) 2022/2557 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους με στόχο τη διασφάλιση της συμμόρφωσης μιας οντότητας που προσδιορίζεται ως κρίσιμη οντότητα βάσει της οδηγίας (ΕΕ) 2022/2557 με τις υποχρεώσεις της παρούσας οδηγίας. Κατά περίπτωση, οι αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2557 θα πρέπει να μπορούν να ζητούν από τις αρμόδιες αρχές δυνάμει της παρούσας οδηγίας να ασκούν τις εποπτικές και εκτελεστικές εξουσίες τους σε σχέση με οντότητα η οποία προσδιορίζεται ως κρίσιμη οντότητα δυνάμει της οδηγίας (ΕΕ) 2022/2557.

10. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας συνεργάζονται με τις σχετικές αρμόδιες αρχές του οικείου κράτους μέλους δυνάμει του κανονισμού (ΕΕ) 2022/2554 Ειδικότερα, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν το φόρουμ εποπτείας που συστάθηκε σύμφωνα με το άρθρο 32 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους που αποσκοπούν στη διασφάλιση της συμμόρφωσης βασικής οντότητας που έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του κανονισμού (ΕΕ) 2022/2554 με τις υποχρεώσεις της παρούσας οδηγίας.

Άρθρο 33

Μέτρα εποπτείας και επιβολής όσον αφορά σημαντικές οντότητες

1. Όταν τους παρέχονται αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες ότι μια σημαντική οντότητα εικάζεται ότι δεν συμμορφώνεται με την παρούσα οδηγία, ιδίως τα άρθρα 21 και 23 αυτής, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές λαμβάνουν μέτρα, εφόσον απαιτείται, μέσω κατασταλτικών εποπτικών μέτρων. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα αυτά είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εξουσιών επιβολής σε σχέση με βασικές οντότητες, έχουν την εξουσία να υποβάλλουν τις εν λόγω οντότητες τουλάχιστον στα ακόλουθα:

α) επιτόπιες επιθεωρήσεις και κατασταλτική εποπτεία εκτός των εγκαταστάσεων, που διενεργούνται από καταρτισμένους επαγγελματίες·

β) στοχευμένους ελέγχους ασφάλειας που διενεργούνται από ανεξάρτητο όργανο ή αρμόδια αρχή·

γ) σαρώσεις ασφαλείας βάσει αντικειμενικών, αμερόληπτων, δίκαιων και διαφανών κριτηρίων αξιολόγησης του κινδύνου, όπου απαιτείται με τη συνεργασία της οικείας οντότητας·

δ) αιτήματα παροχής πληροφοριών αναγκαίων για την αξιολόγηση των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνει η οικεία οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και της συμμόρφωσης με την υποχρέωση διαβίβασης πληροφοριών στις αρμόδιες αρχές σύμφωνα με το άρθρο 27·

ε) αιτήματα για πρόσβαση σε δεδομένα, έγγραφα ή πληροφορίες που είναι αναγκαίες για την εκ μέρους τους εκτέλεση των εποπτικών καθηκόντων τους·

στ) αιτήματα για αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα των ελέγχων ασφάλειας που διενεργούνται από εξουσιοδοτημένο επιθεωρητή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

Οι στοχευμένοι έλεγχοι ασφάλειας που αναφέρονται στο πρώτο εδάφιο στοιχείο β) βασίζονται σε εκτιμήσεις κινδύνου που διενεργούνται από την αρμόδια αρχή ή την ελεγχόμενη οντότητα ή σε άλλες διαθέσιμες πληροφορίες σχετικά με κινδύνους.

Τα αποτελέσματα κάθε στοχευμένου ελέγχου ασφάλειας τίθενται στη διάθεση της αρμόδιας αρχής. Το κόστος του εν λόγω στοχευμένου ελέγχου ασφάλειας που διενεργείται από ανεξάρτητο όργανο καλύπτεται από την ελεγχόμενη οντότητα, εκτός από δεόντως αιτιολογημένες περιπτώσεις για τις οποίες η αρμόδια αρχή αποφασίζει διαφορετικά.

3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχείο δ), ε) ή στ), οι αρμόδιες αρχές δηλώνουν τον σκοπό του αιτήματος και προσδιορίζουν τις ζητούμενες πληροφορίες.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές, κατά την άσκηση των εποπτικών καθηκόντων τους σε σχέση με σημαντικές οντότητες, έχουν την εξουσία τουλάχιστον για τα εξής:

α) να εκδίδουν προειδοποιήσεις σχετικά με τις παραβιάσεις της παρούσας οδηγίας από τις οικείες οντότητες·

β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις οικείες οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή την παράβαση των υποχρεώσεων της παρούσας οδηγίας·

γ) να εντέλλουν τις οικείες οντότητες να παύσουν συμπεριφορά που παραβιάζει την παρούσα οδηγία και να απέχουν από επανάληψη της εν λόγω συμπεριφοράς παραβίασης·

δ) να εντέλλουν τις οικείες οντότητες να διασφαλίσουν ότι τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας συμμορφώνονται με το άρθρο 21 ή να εκπληρώσουν τις υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο άρθρο 23, με συγκεκριμένο τρόπο και εντός καθορισμένου χρονικού διαστήματος·

ε) να εντέλλουν τις οικείες οντότητες να ενημερώσουν τα φυσικά ή νομικά πρόσωπα σε σχέση με τα οποία παρέχουν υπηρεσίες ή ασκούν δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή σχετικά με τη φύση της απειλής, καθώς και σχετικά με τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να λάβουν τα εν λόγω φυσικά ή νομικά πρόσωπα για την αντιμετώπιση της εν λόγω απειλής·

στ) να δίνουν εντολή στις οικείες οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν ως αποτέλεσμα ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να εντέλλουν τις οικείες οντότητες να δημοσιοποιούν πτυχές των παραβιάσεων της παρούσας οδηγίας με συγκεκριμένο τρόπο·

η) να επιβάλλουν, ή ζητούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με το εθνικό δίκαιο, διοικητικού προστίμου δυνάμει του άρθρου 34 επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στα στοιχεία α) έως ζ) της παρούσας παραγράφου.

5. Το άρθρο 32 παράγραφοι 6, 7 και 8 εφαρμόζεται κατ' αναλογία στα μέτρα εποπτείας και επιβολής που προβλέπονται στο παρόν άρθρο για σημαντικές οντότητες.

6. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας συνεργάζονται με τις σχετικές αρμόδιες αρχές του οικείου κράτους μέλους δυνάμει του κανονισμού (ΕΕ) 2022/2554. Ειδικότερα, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους δυνάμει της παρούσας οδηγίας ενημερώνουν το φόρουμ εποπτείας που συστάθηκε σύμφωνα με το άρθρο 32 παράγραφος 1 του κανονισμού (ΕΕ) 2022/2554 κατά την άσκηση των εποπτικών και εκτελεστικών εξουσιών τους που αποσκοπούν στη διασφάλιση της συμμόρφωσης σημαντικής οντότητας που έχει οριστεί ως κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 31 του κανονισμού (ΕΕ) 2022/2554 με τις υποχρεώσεις της παρούσας οδηγίας.

Άρθρο 34

Γενικοί όροι για την επιβολή διοικητικών προστίμων σε βασικές και σημαντικές οντότητες

1. Τα κράτη μέλη διασφαλίζουν ότι τα μέτρα εποπτείας ή επιβολής που επιβάλλονται σε βασικές οντότητες σε σχέση με την παρούσα οδηγία είναι αποτελεσματικά, αναλογικά και αποτρεπτικά, λαμβάνοντας υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

2. Διοικητικά πρόστιμα επιβάλλονται επιπλέον οποιουδήποτε από τα μέτρα που αναφέρονται στο άρθρο 32 παράγραφος 4 στοιχεία α) έως η), στο άρθρο 32 παράγραφος 5 και στο άρθρο 33 παράγραφος 4 στοιχεία α) έως ζ).

3. Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου και τη λήψη απόφασης σχετικά με το ύψος του σε κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη, κατ' ελάχιστον, τα στοιχεία που προβλέπονται στο άρθρο 32 παράγραφος 7.

4. Τα κράτη μέλη διασφαλίζουν ότι, όταν παραβιάζουν το άρθρο 21 ή το άρθρο 23, οι βασικές οντότητες υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 10 000 000 EUR ή κατ' ανώτατο όριο τουλάχιστον 2 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

5. Τα κράτη μέλη διασφαλίζουν ότι, όταν παραβιάζουν το άρθρο 21 ή 23, οι σημαντικές οντότητες υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο τουλάχιστον 7 000 000 EUR ή κατ' ανώτατο όριο τουλάχιστον 1,4 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η σημαντική οντότητα, ανάλογα με το ποιο είναι υψηλότερο.

6. Τα κράτη μέλη μπορούν να προβλέψουν τη δυνατότητα άσκησης εξουσίας επιβολής περιοδικών χρηματικών κυρώσεων προκειμένου να υποχρεώσουν βασική ή σημαντική οντότητα να παύσει μια παράβαση της παρούσας οδηγίας σύμφωνα με προηγούμενη απόφαση της αρμόδιας αρχής.

7. Με την επιφύλαξη των εξουσιών των αρμόδιων αρχών σύμφωνα με τα άρθρα 32 και 33, κάθε κράτος μέλος μπορεί να θεσπίζει κανόνες σχετικά με το εάν και σε ποιο βαθμό μπορούν να επιβληθούν διοικητικά πρόστιμα σε φορείς δημόσιας διοίκησης υποκείμενους στις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

8. Όταν το νομικό σύστημα κράτους μέλους δεν προβλέπει διοικητικά πρόστιμα, το εν λόγω κράτος μέλος διασφαλίζει ότι το παρόν άρθρο εφαρμόζεται κατά τρόπο ώστε το πρόστιμο να κινείται από την αρμόδια αρχή και να επιβάλλεται από τα αρμόδια εθνικά δικαστήρια, διασφαλίζοντας παράλληλα ότι τα εν λόγω ένδικα μέσα είναι αποτελεσματικά και έχουν ισοδύναμο αποτέλεσμα με τα διοικητικά πρόστιμα που επιβάλλονται από τις αρμόδιες αρχές. Σε κάθε περίπτωση, τα πρόστιμα που επιβάλλονται είναι αποτελεσματικά, αναλογικά και αποτρεπτικά. Το κράτος μέλος κοινοποιεί στην Επιτροπή τις διατάξεις των νόμων που θεσπίζει σύμφωνα με την παρούσα παράγραφο, έως τις 17 Οκτωβρίου 2024 και, χωρίς καθυστέρηση, κάθε επακολουθούντα τροποποιητικό νόμο ή τροποποίησή τους.

Άρθρο 35

Παραβάσεις που συνεπάγονται παραβίαση δεδομένων προσωπικού χαρακτήρα

1. Όταν οι αρμόδιες αρχές αντιληφθούν, στο πλαίσιο της εποπτείας ή της επιβολής, ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 21 και 23 της παρούσας οδηγίας μπορεί να συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 σημείο 12) του κανονισμού (ΕΕ) 2016/679, η οποία πρέπει να κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν χωρίς αδικαιολόγητη καθυστέρηση τις εποπτικές αρχές που αναφέρονται στο άρθρο 55 ή 56 του εν λόγω κανονισμού.

2. Όταν οι εποπτικές αρχές που αναφέρονται στο άρθρο 55 ή 56 του κανονισμού (ΕΕ) 2016/679 επιβάλλουν διοικητικό πρόστιμο σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο θ) του εν λόγω κανονισμού, οι αρμόδιες αρχές δεν επιβάλλουν διοικητικό πρόστιμο σύμφωνα με το άρθρο 34 της παρούσας οδηγίας για παράβαση που αναφέρεται στην παράγραφο 1 του παρόντος άρθρου και η οποία απορρέει από την ίδια συμπεριφορά που αποτέλεσε αντικείμενο του διοικητικού προστίμου σύμφωνα με το άρθρο 58 παράγραφος 2 στοιχείο θ) του κανονισμού (ΕΕ) 2016/679. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόσουν τα μέτρα επιβολής που αναφέρονται στο άρθρο 32 παράγραφος 4 στοιχεία α) έως η), στο άρθρο 32 παράγραφος 5 και στο άρθρο 33 παράγραφος 4 στοιχεία α) έως ζ) της παρούσας οδηγίας.

3. Εάν η εποπτική αρχή που είναι αρμόδια δυνάμει του κανονισμού (ΕΕ) 2016/679 είναι εγκατεστημένη σε κράτος μέλος διαφορετικό από την αρμόδια αρχή, η αρμόδια αρχή ενημερώνει την εποπτική αρχή που είναι εγκατεστημένη στο ίδιο κράτος μέλος για την ενδεχόμενη παραβίαση των στοιχείων που αναφέρονται στην παράγραφο 1.

Άρθρο 36

Κυρώσεις

Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις που επιβάλλονται σε περίπτωση παραβιάσεων των εθνικών μέτρων που θεσπίζονται δυνάμει της παρούσας οδηγίας και λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν την εφαρμογή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη κοινοποιούν έως τις 17 Ιανουαρίου 2025 στην Επιτροπή τους εν λόγω κανόνες και τα εν λόγω μέτρα και την ενημερώνουν χωρίς αδικαιολόγητη καθυστέρηση σχετικά με κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 37

Αμοιβαία συνδρομή

1. Όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη ή παρέχει υπηρεσίες σε ένα ή περισσότερα κράτη μέλη και τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, οι αρμόδιες αρχές των ενδιαφερόμενων κρατών μελών συνεργάζονται μεταξύ τους και παρέχουν αμοιβαία συνδρομή, ανάλογα με τις ανάγκες. Η συνεργασία αυτή συνεπάγεται, τουλάχιστον, ότι:

α) οι αρμόδιες αρχές που εφαρμόζουν μέτρα εποπτείας ή επιβολής σε ένα κράτος μέλος ενημερώνουν, μέσω του ενιαίου σημείου επαφής, και διαβουλεύονται με τις αρμόδιες αρχές των άλλων ενδιαφερόμενων κρατών μελών σχετικά με τα μέτρα εποπτείας και επιβολής που λαμβάνονται·

β) μια αρμόδια αρχή μπορεί να ζητήσει από άλλη αρμόδια αρχή να λάβει τα μέτρα εποπτείας ή επιβολής·

γ) μια αρμόδια αρχή, μόλις λάβει τεκμηριωμένο αίτημα από άλλη αρμόδια αρχή, παρέχει στην άλλη αρμόδια αρχή αμοιβαία συνδρομή ανάλογη προς τους πόρους που διαθέτει η ίδια, ώστε τα μέτρα εποπτείας ή επιβολής να μπορούν να εφαρμοστούν με αποτελεσματικό, αποδοτικό και συνεπή τρόπο.

Η αμοιβαία συνδρομή που αναφέρεται στο πρώτο εδάφιο στοιχείο γ) μπορεί να καλύπτει αιτήματα παροχής πληροφοριών και εποπτικά μέτρα, συμπεριλαμβανομένων αιτημάτων για τη διενέργεια επιτόπιων επιθεωρήσεων ή μη επιτόπιας εποπτείας ή στοχευμένων ελέγχων ασφάλειας. Η αρμόδια αρχή στην οποία απευθύνεται αίτημα συνδρομής δεν απορρίπτει την αίτηση αυτή, εκτός εάν διαπιστωθεί ότι δεν είναι αρμόδια να παράσχει τη ζητούμενη συνδρομή, ότι η ζητούμενη συνδρομή δεν είναι ανάλογη προς τα εποπτικά καθήκοντα της αρμόδιας αρχής ή ότι η αίτηση αφορά πληροφορίες ή συνεπάγεται δραστηριότητες οι οποίες, εάν κοινοποιηθούν ή εκτελεστούν, θα ήταν αντίθετες προς τα βασικά συμφέροντα εθνικής ασφάλειας, δημόσιας ασφάλειας ή άμυνας του κράτους μέλους. Πριν απορρίψει το εν λόγω αίτημα, η αρμόδια αρχή διαβουλεύεται με τις άλλες οικείες αρμόδιες αρχές, καθώς και, κατόπιν αιτήματος ενός από τα ενδιαφερόμενα κράτη μέλη, με την Επιτροπή και τον ENISA.

2. Κατά περίπτωση και με κοινή συμφωνία, οι αρμόδιες αρχές διαφόρων κρατών μελών μπορούν να αναλαμβάνουν κοινές εποπτικές ενέργειες.

ΚΕΦΑΛΑΙΟ VIII

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΙ ΕΚΤΕΛΕΣΤΙΚΕΣ ΠΡΑΞΕΙΣ

Άρθρο 38

Άσκηση της εξουσιοδότησης

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

2. Η προβλεπόμενη στο άρθρο 24 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από τις 16 Ιανουαρίου 2023.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 24 παράγραφος 2 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτήν. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.

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

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

6. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 24 παράγραφος 2 τίθεται σε ισχύ εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή από το Συμβούλιο εντός δύο μηνών από την κοινοποίηση της εν λόγω πράξης στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Άρθρο 39

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 παραπομπή στην παρούσα παράγραφο, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.

3. Αν η γνώμη της επιτροπής πρέπει να ληφθεί με γραπτή διαδικασία, η εν λόγω διαδικασία περατώνεται χωρίς αποτέλεσμα, εάν, εντός της προθεσμίας για την έκδοση γνώμης, το αποφασίσει ο πρόεδρος της επιτροπής ή το ζητήσει μέλος της επιτροπής.

ΚΕΦΑΛΑΙΟ IX

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 40

Επανεξέταση

Έως τις 17 Οκτωβρίου 2027 και στη συνέχεια κάθε 36 μήνες, η Επιτροπή προβαίνει σε επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Η έκθεση αξιολογεί ιδίως τη σημασία του μεγέθους των οικείων οντοτήτων, και των τομέων, των υποτομέων και του είδους των οντοτήτων που αναφέρονται στα παραρτήματα I και II για τη λειτουργία της οικονομίας και της κοινωνίας σε σχέση με την κυβερνοασφάλεια. Για τον σκοπό αυτό και με στόχο την περαιτέρω προαγωγή της στρατηγικής και επιχειρησιακής συνεργασίας, η Επιτροπή λαμβάνει υπόψη τις εκθέσεις της Ομάδας Συνεργασίας και του δικτύου CSIRT σχετικά με την πείρα που έχει αποκτηθεί σε στρατηγικό και επιχειρησιακό επίπεδο. Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.

Άρθρο 41

Μεταφορά

1. Έως τις 17 Οκτωβρίου 2024, τα κράτη μέλη θεσπίζουν και δημοσιεύουν τα μέτρα που απαιτούνται προκειμένου να συμμορφωθούν προς την παρούσα οδηγία. Ενημερώνουν αμέσως την Επιτροπή σχετικά.

Εφαρμόζουν τα μέτρα αυτά από τις 18 Οκτωβρίου 2024.

2. Οι διατάξεις που αναφέρονται στην παράγραφο 1, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν παραπομπή στην παρούσα οδηγία ή συνοδεύονται από την παραπομπή αυτή κατά την επίσημη δημοσίευσή τους. Ο τρόπος της παραπομπής αυτής καθορίζεται από τα κράτη μέλη.

Άρθρο 42

Τροποποιήσεις του κανονισμού (ΕΕ) αριθ. 910/2014

Στον κανονισμό (ΕΕ) αριθ. 910/2014, το άρθρο 19 απαλείφεται από τις 18 Οκτωβρίου 2024.

Άρθρο 43

Τροποποίηση της οδηγίας (ΕΕ) 2018/1972

Στην οδηγία (ΕΕ) 2018/1972, τα άρθρα 40 και 41 απαλείφονται από τις 18 Οκτωβρίου 2024.

Άρθρο 44

Κατάργηση

Η οδηγία (ΕΕ) 2016/1148 καταργείται από τις 18 Οκτωβρίου 2024.

Οι παραπομπές στην καταργούμενη οδηγία νοούνται ως παραπομπές στην παρούσα οδηγία σύμφωνα με τον πίνακα αντιστοιχίας που παρατίθεται στο παράρτημα III.

Άρθρο 45

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 46

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Στρασβούργο, 14 Δεκεμβρίου 2022.

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*
R. METSOLA	M. BEK

ΠΑΡΑΡΤΗΜΑ Ι

ΤΟΜΕΙΣ ΥΨΗΛΗΣ ΚΡΙΣΙΜΟΤΗΤΑΣ

Τομέας	Υποτομέας	Είδος οντότητας
1. Ενέργεια	α) Ηλεκτρική ενέργεια	— Επιχειρήσεις ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 57) της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1], οι οποίες ασκούν τη δραστηριότητα «προμήθεια», όπως ορίζεται στο άρθρο 2 σημείο 12) της εν λόγω οδηγίας
		— Διαχειριστές συστημάτων διανομής όπως ορίζονται στο άρθρο 2 σημείο 29) της οδηγίας (ΕΕ) 2019/944
		— Διαχειριστές συστημάτων μεταφοράς όπως ορίζονται στο άρθρο 2 σημείο 35) της οδηγίας (ΕΕ) 2019/944
		— Παραγωγοί όπως ορίζονται στο άρθρο 2 σημείο 38) της οδηγίας (ΕΕ) 2019/944
		— Ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [2] — Συμμετέχοντες στην αγορά, όπως ορίζονται στο άρθρο 2 σημείο 25) του κανονισμού (ΕΕ) 2019/943, οι οποίοι παρέχουν υπηρεσίες συγκέντρωσης, απόκρισης ζήτησης ή αποθήκευσης ενέργειας, όπως ορίζονται στο άρθρο 2 σημεία 18), 20) και 59) της οδηγίας (ΕΕ) 2019/944 — Διαχειριστές σημείου επαναφόρτισης που είναι υπεύθυνοι για τη διαχείριση και τη λειτουργία σημείου επαναφόρτισης, το οποίο παρέχει υπηρεσία επαναφόρτισης στους τελικούς χρήστες, μεταξύ άλλων εξ ονόματος και για λογαριασμό παρόχου υπηρεσιών κινητικότητας
	β) Τηλεθέρμανση και τηλεψύξη	— Διαχειριστές τηλεθέρμανσης ή τηλεψύξης, όπως ορίζονται στο άρθρο 2 σημείο 19) της οδηγίας (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [3]
	γ) Πετρέλαιο	— Διαχειριστές αγωγών μεταφοράς πετρελαίου
		— Διαχειριστές παραγωγής πετρελαίου, εγκαταστάσεων διύλισης και επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου
		— Κεντρικοί φορείς διατήρησης αποθεμάτων, όπως ορίζονται στο άρθρο 2 στοιχείο στ) της οδηγίας 2009/119/ΕΚ του Συμβουλίου [4]
	δ) Αέριο	— Επιχειρήσεις προμήθειας όπως ορίζονται στο άρθρο 2 σημείο 8) της οδηγίας 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [5]
		— Διαχειριστές συστημάτων διανομής όπως ορίζονται στο άρθρο 2 σημείο 6) της οδηγίας 2009/944/ΕΚ
		— Διαχειριστές συστημάτων μεταφοράς όπως ορίζονται στο άρθρο 2 σημείο 4) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστημάτων αποθήκευσης όπως ορίζονται στο άρθρο 2 σημείο 10) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές συστημάτων ΥΦΑ όπως ορίζονται στο άρθρο 2 σημείο 12) της οδηγίας 2009/73/ΕΚ
		— Επιχειρήσεις φυσικού αερίου όπως ορίζονται στο άρθρο 2 σημείο 1) της οδηγίας 2009/73/ΕΚ
		— Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου
	ε) Υδρογόνο	— Διαχειριστές παραγωγής, αποθήκευσης και μεταφοράς υδρογόνου

Τομέας	Υποτομέας	Είδος οντότητας
2. Μεταφορές	α) Εναέριες	— Αερομεταφορείς όπως ορίζονται στο άρθρο 3 σημείο 4) του κανονισμού (ΕΚ) αριθ. 300/2008, που χρησιμοποιούνται για εμπορικούς σκοπούς
		— Φορείς διαχείρισης αερολιμένα, όπως ορίζονται στο άρθρο 2 σημείο 2) της οδηγίας 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), αερολιμένες όπως ορίζονται στο άρθρο 2 σημείο 2) της εν λόγω οδηγίας, συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο παράρτημα ΙΙ τμήμα 2 του κανονισμού (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός αερολιμένων
		— Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8])
	β) Σιδηροδρομικές	— Διαχειριστές υποδομής όπως ορίζονται στο άρθρο 3 σημείο 2) της οδηγίας 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9])
		— Σιδηροδρομικές επιχειρήσεις, όπως ορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2012/34/ΕΕ, συμπεριλαμβανομένων των φορέων εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών όπως ορίζονται στο άρθρο 3 σημείο 12) της εν λόγω οδηγίας
	γ) Πλωτές	— Εσωτερικές πλωτές, θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εμπορευμάτων, όπως ορίζονται για τις θαλάσσιες μεταφορές στο παράρτημα Ι του κανονισμού (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10]), μη συμπεριλαμβανομένων των μεμονωμένων πλοίων που χρησιμοποιούνται από τις εταιρείες αυτές
		— Διαχειριστικοί φορείς των λιμένων, όπως ορίζονται στο άρθρο 3 σημείο 1) της οδηγίας 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]), συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων όπως ορίζονται στο άρθρο 2 σημείο 11) του κανονισμού (ΕΚ) αριθ. 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός λιμένων
		— Φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων (VTS), όπως ορίζονται στο άρθρο 3 στοιχείο ιε) της οδηγίας 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12])
	δ) Οδικές	— Οδικές αρχές, όπως ορίζονται στο άρθρο 2 σημείο 12) του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2015/962 της Επιτροπής ([13]), αρμόδιες για τον έλεγχο της διαχείρισης της κυκλοφορίας, εξαιρουμένων των δημόσιων φορέων για τους οποίους η διαχείριση της κυκλοφορίας ή η λειτουργία ευφυών συστημάτων μεταφορών αποτελεί μη ουσιώδες μέρος της γενικής δραστηριότητάς τους
		— Φορείς εκμετάλλευσης συστημάτων ευφυών μεταφορών (ITS), όπως ορίζονται στο άρθρο 4 σημείο 1) της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([14])
3. Τράπεζες		Πιστωτικά ιδρύματα όπως ορίζονται στο άρθρο 4 σημείο 1) του κανονισμού (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15])
4. Υποδομές χρηματοπιστωτικών αγορών		— Φορείς εκμετάλλευσης τόπων διαπραγμάτευσης, όπως ορίζονται στο άρθρο 4 σημείο 24) της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16])
		— Κεντρικοί αντισυμβαλλόμενοι, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([17])

Τομέας	Υποτομέας	Είδος οντότητας
5. Υγεία		— Πάροχοι υγειονομικής περίθαλψης, όπως ορίζονται στο άρθρο 3 στοιχείο ζ) της οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18])
		— Εργαστήρια αναφοράς της ΕΕ που αναφέρονται στο άρθρο 15 του κανονισμού (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([19])
		— Οντότητες που πραγματοποιούν δραστηριότητες έρευνας και ανάπτυξης για φάρμακα, που αναφέρονται στο άρθρο 1 σημείο 2) της οδηγίας 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([20]) — Οντότητες που παρασκευάζουν βασικά φαρμακευτικά προϊόντα και φαρμακευτικά σκευάσματα που αναφέρονται στον τομέα Γ κλάδο 21 της NACE αναθ. 2 — Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα που θεωρούνται κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας (κατάλογος τεχνολογικών προϊόντων κρίσιμης σημασίας κατά τη διάρκεια κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας) κατά την έννοια του άρθρου 22 του κανονισμού (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([21])
6. Πόσιμο νερό		Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης όπως ορίζονται στο άρθρο 2 σημείο 1) στοιχείο α) της οδηγίας (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([22]), εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών
7. Λύματα		Επιχειρήσεις συλλογής, διάθεσης ή επεξεργασίας αστικών, οικιακών ή βιομηχανικών λυμάτων που αναφέρονται στο άρθρο 2 σημεία 1), 2) και 3) της οδηγίας 91/271/ΕΟΚ του Συμβουλίου ([23]), εξαιρουμένων επιχειρήσεων για τις οποίες η συλλογή, η διάθεση ή η επεξεργασία αστικών, οικιακών ή βιομηχανικών λυμάτων αποτελεί επουσιώδες μέρος της γενικής τους δραστηριότητας.
8. Ψηφιακές υποδομές		— Πάροχοι σημείων ανταλλαγής κίνησης διαδικτύου
		— Πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), εξαιρουμένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας
		— Μητρώα ονομάτων τομέα ανώτατου επιπέδου (TLD)
		— Πάροχοι υπηρεσιών υπολογιστικού νέφους
		— Πάροχοι υπηρεσιών κέντρου δεδομένων
		— Πάροχοι δικτύων διανομής περιεχομένου
		— Πάροχοι υπηρεσιών εμπιστοσύνης·
		— Πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών
		— Πάροχοι δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών
9. Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)		— Πάροχοι διαχειριζόμενων υπηρεσιών — Πάροχοι διαχειριζόμενων υπηρεσιών ασφαλείας

Τομέας	Υποτομέας	Είδος οντότητας
10. Οντότητες δημόσιας διοίκησης		— Οντότητες δημόσιας διοίκησης της κυβέρνησης όπως ορίζονται από το κράτος μέλος σύμφωνα με το εθνικό δίκαιο
		— Οντότητες δημόσιας διοίκησης σε περιφερειακό επίπεδο όπως ορίζονται από το κράτος μέλος σύμφωνα με το εθνικό δίκαιο
11. Διάστημα		Φορείς εκμετάλλευσης επίγειας υποδομής, ιδιοκτησίας, διαχείρισης και εκμετάλλευσης από κράτη μέλη ή ιδιωτικούς φορείς, οι οποίοι υποστηρίζουν την παροχή διαστημικών υπηρεσιών, εξαιρουμένων των παρόχων δημόσιων δικτύων ηλεκτρονικών επικοινωνιών

(1) Οδηγία (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125).

(2) Κανονισμός (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας (ΕΕ L 158 της 14.6.2019, σ. 54).

(3) Οδηγία (ΕΕ) 2018/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για την προώθηση της χρήσης ενέργειας από ανανεώσιμες πηγές (ΕΕ L 328 της 21.12.2018, σ. 82).

(4) Οδηγία 2009/119/ΕΚ του Συμβουλίου, της 14ης Σεπτεμβρίου 2009, σχετικά με υποχρέωση διατήρησης ενός ελάχιστου επιπέδου αποθεμάτων αργού πετρελαίου ή/και προϊόντων πετρελαίου από τα κράτη μέλη (ΕΕ L 265 της 9.10.2009, σ. 9).

(5) Οδηγία 2009/73/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουλίου 2009, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά φυσικού αερίου και την κατάργηση της οδηγίας 2003/55/ΕΚ (ΕΕ L 211 της 14.8.2009, σ. 94).

(6) Οδηγία 2009/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, για τα αερολιμενικά τέλη (ΕΕ L 70 της 14.3.2009, σ. 11).

(7) Κανονισμός (ΕΕ) αριθ. 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2013, περί των προσανατολισμών της Ένωσης για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών και για την κατάργηση της απόφασης αριθ. 661/2010/ΕΕ (ΕΕ L 348 της 20.12.2013, σ. 1).

(8) Κανονισμός (ΕΚ) αριθ. 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη χάραξη του πλαισίου για τη δημιουργία του Ενιαίου Ευρωπαϊκού Ουρανού (κανονισμός-πλαίσιο) (ΕΕ L 96 της 31.3.2004, σ. 1).

(9) Οδηγία 2012/34/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Νοεμβρίου 2012, για τη δημιουργία ενιαίου ευρωπαϊκού σιδηροδρομικού χώρου (ΕΕ L 343 της 14.12.2012, σ. 32).

(10) Κανονισμός (ΕΚ) αριθ. 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 31ης Μαρτίου 2004, για τη βελτίωση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (ΕΕ L 129 της 29.4.2004, σ. 6).

(11) Οδηγία 2005/65/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2005, σχετικά με την ενίσχυση της ασφαλείας των λιμένων (ΕΕ L 310 της 25.11.2005, σ. 28).

(12) Οδηγία 2002/59/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Ιουνίου 2002, για τη δημιουργία κοινοτικού συστήματος παρακολούθησης της κυκλοφορίας των πλοίων και ενημέρωσης και την κατάργηση της οδηγίας 93/75/ΕΟΚ του Συμβουλίου (ΕΕ L 208 της 5.8.2002, σ. 10).

(13) Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2015/962 της Επιτροπής, της 18ης Δεκεμβρίου 2014, για τη συμπλήρωση της οδηγίας 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την παροχή σε επίπεδο Ένωσης υπηρεσιών πληροφόρησης για την κυκλοφορία σε πραγματικό χρόνο (ΕΕ L 157 της 23.6.2015, σ. 21).

(14) Οδηγία 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Ιουλίου 2010, περί πλαισίου ανάπτυξης των Συστημάτων Ευφυών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς (ΕΕ L 207 της 6.8.2010, σ. 1).

(15) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

(16) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349).

(17) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201 της 27.7.2012, σ. 1).

(18) Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2011, περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (ΕΕ L 88 της 4.4.2011, σ. 45).

(19) Κανονισμός (ΕΕ) 2022/2371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Νοεμβρίου 2022, σχετικά με σοβαρές διασυνοριακές απειλές κατά της υγείας και για την κατάργηση της απόφασης αριθ. 1082/2013/ΕΕ (ΕΕ L 314 της 6.12.2022, σ. 26).

(20) Οδηγία 2001/83/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Νοεμβρίου 2001, περί κοινοτικού κώδικος για τα φάρμακα που προορίζονται για ανθρώπινη χρήση (ΕΕ L 311 της 28.11.2001, σ. 67).

(21) Κανονισμός (ΕΕ) 2022/123 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Ιανουαρίου 2022 σχετικά με την ενίσχυση του ρόλου του Ευρωπαϊκού Οργανισμού Φαρμάκων όσον αφορά την ετοιμότητα έναντι κρίσεων και τη διαχείριση κρίσεων για τα φάρμακα και τα ιατροτεχνολογικά προϊόντα (ΕΕ L 20 της 31.1.2022, σ. 1).

(22) Οδηγία (ΕΕ) 2020/2184 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Δεκεμβρίου 2020, σχετικά με την ποιότητα του νερού ανθρώπινης κατανάλωσης (ΕΕ L 435 της 23.12.2020, σ. 1).

(23) Οδηγία 91/271/ΕΟΚ του Συμβουλίου, της 21ης Μαΐου 1991, για την επεξεργασία των αστικών λυμάτων (ΕΕ L 135 της 30.5.1991, σ. 40).

ΠΑΡΑΡΤΗΜΑ II

ΑΛΛΟΙ ΚΡΙΣΙΜΟΙ ΤΟΜΕΙΣ

Τομέας	Υποτομέας	Είδος οντότητας
1. Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών		Φορείς παροχής ταχυδρομικών υπηρεσιών όπως ορίζονται στο άρθρο 2 σημείο 1α) της οδηγίας 97/67/ΕΚ, συμπεριλαμβανομένων παρόχων υπηρεσιών ταχυμεταφορών
2. Διαχείριση αποβλήτων		Επιχειρήσεις διαχείρισης αποβλήτων όπως ορίζονται στο άρθρο 3 σημείο 9) της οδηγίας 2008/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), με εξαίρεση τις επιχειρήσεις για τις οποίες η διαχείριση αποβλήτων δεν αποτελεί την κύρια οικονομική δραστηριότητα
3. Παρασκευή, παραγωγή και διανομή χημικών προϊόντων		Επιχειρήσεις που ασχολούνται με την παρασκευή ουσιών και τη διανομή ουσιών ή μειγμάτων, όπως αναφέρεται στο άρθρο 3 σημεία 9) και 14) του κανονισμού (ΕΚ) αριθ. 1907/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), και επιχειρήσεις που παράγουν αντικείμενα, όπως ορίζονται στο άρθρο 3 σημείο 3) του εν λόγω κανονισμού, από ουσίες ή μείγματα
4. Παραγωγή, μεταποίηση και διανομή τροφίμων		Επιχειρήσεις τροφίμων, όπως ορίζονται στο άρθρο 3 σημείο 2) του κανονισμού (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), οι οποίες δραστηριοποιούνται στη χονδρική διανομή και τη βιομηχανική παραγωγή και μεταποίηση
5. Κατασκευαστικός τομέας	α) Κατασκευή ιατροτεχνολογικών προϊόντων και in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων	Οντότητες που κατασκευάζουν ιατροτεχνολογικά προϊόντα, όπως ορίζονται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), και οντότητες που κατασκευάζουν in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα, όπως ορίζονται στο άρθρο 2 σημείο 2) του κανονισμού (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), εξαιρουμένων των οντοτήτων που κατασκευάζουν ιατροτεχνολογικά προϊόντα που αναφέρονται στο παράρτημα I σημείο 5 πέμπτη περίπτωση της παρούσας οδηγίας
	β) Κατασκευή προϊόντων υπολογιστών, ηλεκτρονικών και οπτικών προϊόντων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 26 της NACE αναθ. 2
	γ) Κατασκευή ηλεκτρολογικού εξοπλισμού	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 27 της NACE αναθ. 2
	δ) Κατασκευή μηχανημάτων και εξοπλισμού π.δ.κ.α.	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 28 της NACE αναθ. 2
	ε) Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 29 της NACE αναθ. 2
	στ) Κατασκευή άλλου εξοπλισμού μεταφορών	Επιχειρήσεις που ασκούν οικονομικές δραστηριότητες που αναφέρονται στον τομέα Γ κλάδο 30 της NACE αναθ. 2

Τομέας	Υποτομέας	Είδος οντότητας
6. Ψηφιακοί πάροχοι		— Πάροχοι επιγραμμικών αγορών
		— Πάροχοι επιγραμμικών μηχανών αναζήτησης
		— Πάροχοι πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης
7. Έρευνα		Οργανισμοί έρευνας

([1]) Οδηγία 2008/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Νοεμβρίου 2008, για τα απόβλητα και την κατάργηση ορισμένων οδηγιών (ΕΕ L 312 της 22.11.2008, σ. 3).

([2]) Κανονισμός (ΕΚ) αριθ. 1907/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την καταχώριση, την αξιολόγηση, την αδειοδότηση και τους περιορισμούς των χημικών προϊόντων (REACH) και για την ίδρυση του Ευρωπαϊκού Οργανισμού Χημικών Προϊόντων καθώς και για την τροποποίηση της οδηγίας 1999/45/ΕΚ και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 793/93 του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 1488/94 της Επιτροπής καθώς και της οδηγίας 76/769/ΕΟΚ του Συμβουλίου και των οδηγιών της Επιτροπής 91/155/ΕΟΚ, 93/67/ΕΟΚ, 93/105/ΕΚ και 2000/21/ΕΚ (ΕΕ L 396 της 30.12.2006, σ. 1).

([3]) Κανονισμός (ΕΚ) αριθ. 178/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28ης Ιανουαρίου 2002, για τον καθορισμό των γενικών αρχών και απαιτήσεων της νομοθεσίας για τα τρόφιμα, για την ίδρυση της Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων και τον καθορισμό διαδικασιών σε θέματα ασφαλείας των τροφίμων (ΕΕ L 31 της 1.2.2002, σ. 1).

([4]) Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ (ΕΕ L 117 της 5.5.2017, σ. 1)

([5]) Κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα και για την κατάργηση της οδηγίας 98/79/ΕΚ και της απόφασης 2010/227/ΕΕ της Επιτροπής (ΕΕ L 117 της 5.5.2017, σ. 176).

ΠΑΡΑΡΤΗΜΑ III

ΠΙΝΑΚΑΣ ΑΝΤΙΣΤΟΙΧΙΑΣ

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Άρθρο 1 παράγραφος 1	Άρθρο 1 παράγραφος 1
Άρθρο 1 παράγραφος 2	Άρθρο 1 παράγραφος 2
Άρθρο 1 παράγραφος 3	-
Άρθρο 1 παράγραφος 4	Άρθρο 2 παράγραφος 12
Άρθρο 1 παράγραφος 5	Άρθρο 2 παράγραφος 13
Άρθρο 1 παράγραφος 6	Άρθρο 2 παράγραφοι 6 και 11
Άρθρο 1 παράγραφος 7	Άρθρο 4
Άρθρο 2	Άρθρο 2 παράγραφος 14
Άρθρο 3	Άρθρο 5
Άρθρο 4	Άρθρο 6
Άρθρο 5	-
Άρθρο 6	-
Άρθρο 7 παράγραφος 1	Άρθρο 7 παράγραφοι 1 και 2
Άρθρο 7 παράγραφος 2	Άρθρο 7 παράγραφος 4
Άρθρο 7 παράγραφος 3	Άρθρο 7 παράγραφος 3
Άρθρο 8 παράγραφοι 1 έως 5	Άρθρο 8 παράγραφοι 1 έως 5
Άρθρο 8 παράγραφος 6	Άρθρο 13 παράγραφος 4
Άρθρο 8 παράγραφος 7	Άρθρο 8 παράγραφος 6
Άρθρο 9 παράγραφοι 1, 2 και 3	Άρθρο 10 παράγραφοι 1, 2 και 3
Άρθρο 9 παράγραφος 4	Άρθρο 10 παράγραφος 9
Άρθρο 9 παράγραφος 5	Άρθρο 10 παράγραφος 10
Άρθρο 10 παράγραφοι 1, 2 και 3 πρώτο εδάφιο	Άρθρο 13 παράγραφοι 1, 2 και 3
Άρθρο 10 παράγραφος 3 δεύτερο εδάφιο	Άρθρο 23 παράγραφος 9
Άρθρο 11 παράγραφος 1	Άρθρο 14 παράγραφοι 1 και 2
Άρθρο 11 παράγραφος 2	Άρθρο 14 παράγραφος 3
Άρθρο 11 παράγραφος 3	Άρθρο 14 παράγραφος 4 πρώτο εδάφιο στοιχεία α) έως η) και παράγραφος 7
Άρθρο 11 παράγραφος 4	Άρθρο 14 παράγραφος 4 πρώτο εδάφιο στοιχείο η) και δεύτερο εδάφιο
Άρθρο 11 παράγραφος 5	Άρθρο 14 παράγραφος 8
Άρθρο 12 παράγραφοι 1 έως 5	Άρθρο 15 παράγραφοι 1 έως 5
Άρθρο 13	Άρθρο 17
Άρθρο 14 παράγραφοι 1 και 2	Άρθρο 21 παράγραφοι 1 έως 4
Άρθρο 14 παράγραφος 3	Άρθρο 23 παράγραφος 1
Άρθρο 14 παράγραφος 4	Άρθρο 23 παράγραφος 3
Άρθρο 14 παράγραφος 5	Άρθρο 23 παράγραφοι 5, 6 και 8

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Άρθρο 14 παράγραφος 6	Άρθρο 23 παράγραφος 7
Άρθρο 14 παράγραφος 7	Άρθρο 23 παράγραφος 11
Άρθρο 15 παράγραφος 1	Άρθρο 31 παράγραφος 1
Άρθρο 15 παράγραφος 2 πρώτο εδάφιο στοιχείο α)	Άρθρο 32 παράγραφος 2 στοιχείο ε)
Άρθρο 15 παράγραφος 2 πρώτο εδάφιο στοιχείο β)	Άρθρο 32 παράγραφος 2 στοιχείο ζ)
Άρθρο 15 παράγραφος 2 δεύτερο εδάφιο	Άρθρο 32 παράγραφος 3
Άρθρο 15 παράγραφος 3	Άρθρο 32 παράγραφος 4 στοιχείο β)
Άρθρο 15 παράγραφος 4	Άρθρο 31 παράγραφος 3
Άρθρο 16 παράγραφοι 1 και 2	Άρθρο 21 παράγραφοι 1 έως 4
Άρθρο 16 παράγραφος 3	Άρθρο 23 παράγραφος 1
Άρθρο 16 παράγραφος 4	Άρθρο 23 παράγραφος 3
Άρθρο 16 παράγραφος 5	-
Άρθρο 16 παράγραφος 6	Άρθρο 23 παράγραφος 6
Άρθρο 16 παράγραφος 7	Άρθρο 23 παράγραφος 7
Άρθρο 16 παράγραφοι 8 και 9	Άρθρο 21 παράγραφος 5 και άρθρο 23 παράγραφος 11
Άρθρο 16 παράγραφος 10	-
Άρθρο 16 παράγραφος 11	Άρθρο 2 παράγραφοι 1, 2 και 3
Άρθρο 17 παράγραφος 1	Άρθρο 33 παράγραφος 1
Άρθρο 17 παράγραφος 2 στοιχείο α)	Άρθρο 32 παράγραφος 2 στοιχείο ε)
Άρθρο 17 παράγραφος 2 στοιχείο β)	Άρθρο 32 παράγραφος 4 στοιχείο β)
Άρθρο 17 παράγραφος 3	Άρθρο 37 παράγραφος 1 στοιχεία α) και β)
Άρθρο 18 παράγραφος 1	Άρθρο 26 παράγραφος 1 στοιχείο β) και παράγραφος 2
Άρθρο 18 παράγραφος 2	Άρθρο 26 παράγραφος 3
Άρθρο 18 παράγραφος 3	Άρθρο 26 παράγραφος 4
Άρθρο 19	Άρθρο 25
Άρθρο 20	Άρθρο 30
Άρθρο 21	Άρθρο 36
Άρθρο 22	Άρθρο 39
Άρθρο 23	Άρθρο 40
Άρθρο 24	-
Άρθρο 25	Άρθρο 41
Άρθρο 26	Άρθρο 45
Άρθρο 27	Άρθρο 46
Παράρτημα 1 σημείο 1	Άρθρο 11 παράγραφος 1
Παράρτημα Ι σημείο 2 στοιχείο α) σημεία i) έως iv)	Άρθρο 11 παράγραφος 2 στοιχεία α) έως δ)

Οδηγία (ΕΕ) 2016/1148	Παρούσα οδηγία
Παράρτημα I σημείο 2 στοιχείο α) σημείο v)	Άρθρο 11 παράγραφος 2 στοιχείο στ)
Παράρτημα I σημείο 2 στοιχείο β)	Άρθρο 11 παράγραφος 4
Παράρτημα I σημείο 2 στοιχείο γ) σημεία i) και ii)	Άρθρο 11 παράγραφος 5 στοιχείο α)
Παράρτημα II	Παράρτημα I
Παράρτημα III σημεία 1 και 2	Παράρτημα II σημείο 6
Παράρτημα III σημείο 3	Παράρτημα I σημείο 8