ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Πρόταση

ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

- **Αιτιολόγηση και στόχοι της πρότασης**

Η παρούσα πρόταση αποτελεί μέρος δέσμης μέτρων για την περαιτέρω βελτίωση της ανθεκτικότητας και των ικανοτήτων αντιμετώπισης περιστατικών των δημόσιων και ιδιωτικών φορέων, των αρμόδιων αρχών, και της Ένωσης συνολικά στον τομέα της κυβερνοασφάλειας και της προστασίας των κρίσιμων υποδομών. Η πρόταση συνάδει με τις προτεραιότητες της Επιτροπής να προετοιμάσει την Ευρώπη για την ψηφιακή εποχή και να οικοδομήσει μια οικονομία έτοιμη να αντιμετωπίσει το μέλλον, στην υπηρεσία των πολιτών. Στο πλαίσιο της αντίδρασης της Επιτροπής στην κρίση COVID-19 η κυβερνοασφάλεια συνιστά προτεραιότητα. Η δέσμη μέτρων περιλαμβάνει μια νέα στρατηγική για την κυβερνοασφάλεια για την ενίσχυση της στρατηγικής αυτονομίας της Ένωσης με σκοπό τη βελτίωση της ανθεκτικότητας και της συλλογικής αντίδρασής της και την οικοδόμηση ενός ανοικτού και παγκόσμιου διαδικτύου. Τέλος, η δέσμη μέτρων περιλαμβάνει πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων φορέων εκμετάλλευσης βασικών υπηρεσιών, η οποία αποσκοπεί στον μετριασμό των υλικών απειλών κατά τέτοιων φορέων εκμετάλλευσης.

Η παρούσα πρόταση έχει ως βάση και καταργεί την οδηγία (ΕΕ) 2016/1148 για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (στο εξής: οδηγία NIS), η οποία αποτελεί την πρώτη νομοθετική πράξη της ΕΕ για την κυβερνοασφάλεια και προβλέπει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην Ένωση. Η οδηγία NIS, 1) συνέβαλε στη βελτίωση των ικανοτήτων κυβερνοασφάλειας σε εθνικό επίπεδο απαιτώντας από τα κράτη μέλη να θεσπίσουν εθνικές στρατηγικές κυβερνοασφάλειας και να ορίσουν αρχές κυβερνοασφάλειας, 2) ενέτεινε τη συνεργασία μεταξύ των κρατών μελών σε επίπεδο Ένωσης με τη δημιουργία διαφόρων φόρουμ που προάγουν την ανταλλαγή στρατηγικών και επιχειρησιακών πληροφοριών, και 3) βελτίωσε την κυβερνοανθεκτικότητα δημόσιων και ιδιωτικών οντοτήτων σε επτά ειδικούς τομείς (ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγειονομική περίθαλψη, παροχή και διανομή πόσιμου νερού, ψηφιακές υποδομές) και σε τρεις ψηφιακές υπηρεσίες (επιγραμμικές αγορές, επιγραμμικές μηχανές αναζήτησης, υπηρεσίες νεφοϋπολογιστικής), απαιτώντας από τα κράτη μέλη να μεριμνούν ώστε οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών να τηρούν τις απαιτήσεις κυβερνοασφάλειας και να αναφέρουν τυχόν περιστατικά.

Η πρόταση εκσυγχρονίζει το υφιστάμενο νομικό πλαίσιο, λαμβάνοντας υπόψη την αυξημένη ψηφιοποίηση της εσωτερικής αγοράς τα τελευταία χρόνια και το εξελισσόμενο τοπίο των απειλών για την κυβερνοασφάλεια. Και οι δύο αυτές εξελίξεις έχουν επιταχυνθεί περαιτέρω μετά την έναρξη της κρίσης της COVID-19. Η πρόταση αντιμετωπίζει επίσης αρκετές αδυναμίες οι οποίες δεν επέτρεψαν να αξιοποιηθεί πλήρως το δυναμικό της οδηγίας NIS.

Παρά τα αξιοσημείωτα επιτεύγματά της, η οδηγία NIS —η οποία άνοιξε το δρόμο για μια σημαντική αλλαγή νοοτροπίας ως προς τη θεσμική και κανονιστική προσέγγιση της κυβερνοασφάλειας σε πολλά κράτη μέλη— έχει δείξει και τα όριά της. Ο ψηφιακός μετασχηματισμός της κοινωνίας (που εντάθηκε από την κρίση της COVID-19), έχει διευρύνει το τοπίο των απειλών και δημιουργεί νέες προκλήσεις, οι οποίες απαιτούν προσαρμοσμένες και καινοτόμες απαντήσεις. Ο αριθμός των κυβερνοεπιθέσεων εξακολουθεί να αυξάνεται, καθώς εξαπολύονται ολοένα και πιο εξελιγμένες επιθέσεις από ένα ευρύ φάσμα πηγών εντός και εκτός της ΕΕ.

Από την αξιολόγηση της λειτουργίας της οδηγίας NIS, που έγινε στο πλαίσιο της εκτίμησης επιπτώσεων, εντοπίστηκαν τα ακόλουθα ζητήματα: 1) χαμηλό επίπεδο

κυβερνοανθεκτικότητας των επιχειρήσεων που δραστηριοποιούνται στην ΕΕ, 2) διαφορές όσον αφορά την ανθεκτικότητα μεταξύ κρατών μελών και τομέων, και 3) χαμηλό επίπεδο κοινής επίγνωσης της κατάστασης και έλλειψη κοινής αντιμετώπισης των κρίσεων. Για παράδειγμα, ορισμένα μεγάλα νοσοκομεία σε ένα κράτος μέλος δεν εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS και, ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν τα ανάλογα μέτρα ασφάλειας, ενώ σε ένα άλλο κράτος μέλος σχεδόν όλοι οι πάροχοι υγειονομικής περίθαλψης στη χώρα καλύπτονται από τις απαιτήσεις ασφάλειας της οδηγίας NIS.

Δεδομένου ότι αποτελεί πρωτοβουλία στο πλαίσιο του προγράμματος βελτίωσης της καταλληλότητας του κανονιστικού πλαισίου (REFIT), η πρόταση αποσκοπεί στη μείωση του κανονιστικού φόρτου για τις αρμόδιες αρχές και του κόστους συμμόρφωσης για τις δημόσιες και ιδιωτικές οντότητες. Ειδικότερα, αυτό επιτυγχάνεται με την κατάργηση της υποχρέωσης των αρμόδιων αρχών να προσδιορίζουν τους φορείς εκμετάλλευσης βασικών υπηρεσιών και με την αύξηση του επιπέδου εναρμόνισης των απαιτήσεων ασφάλειας και αναφοράς περιστατικών για τη διευκόλυνση της κανονιστικής συμμόρφωσης των οντοτήτων που παρέχουν διασυνοριακές υπηρεσίες. Ταυτοχρόνως, στις αρμόδιες αρχές θα ανατεθούν και ορισμένα νέα καθήκοντα, όπως η εποπτεία οντοτήτων σε τομείς που μέχρι στιγμής δεν καλύπτονται από την οδηγία NIS.

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

Η παρούσα πρόταση αποτελεί μέρος ενός ευρύτερου συνόλου υφιστάμενων νομικών μέσων και επικείμενων πρωτοβουλιών σε επίπεδο Ένωσης που αποσκοπούν στην αύξηση της ανθεκτικότητας των δημόσιων και ιδιωτικών οντοτήτων έναντι απειλών.

Στον τομέα της κυβερνοασφάλειας, πρόκειται κυρίως για την οδηγία (ΕΕ) 2018/1972 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (της οποίας οι διατάξεις που αφορούν την κυβερνοασφάλεια θα αντικατασταθούν από τις διατάξεις της παρούσας πρότασης), και για την πρόταση κανονισμού σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα [COM(2020) 595 final], η οποία θα θεωρείται lex specialis σε σχέση με την παρούσα πρόταση, άπαξ και τεθούν σε ισχύ αμφότερες οι πράξεις.

Στον τομέα της υλικής ασφάλειας, η πρόταση συμπληρώνει την πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων, η οποία αναθεωρεί την οδηγία 2008/114/ΕΚ σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (οδηγία ECI), η οποία θεσπίζει ενωσιακή διαδικασία για τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και καθορίζει προσέγγιση για τη βελτίωση της προστασίας τους. Τον Ιούλιο του 2020, η Επιτροπή ενέκρινε τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας[1], με την οποία αναγνωρίζεται η αυξανόμενη διασύνδεση και αλληλεξάρτηση μεταξύ υλικών και ψηφιακών υποδομών. Η στρατηγική υπογράμμισε την ανάγκη για μια πιο συνεκτική και συνεπή προσέγγιση μεταξύ της οδηγίας ECI και της οδηγίας (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων σε ολόκληρη την Ένωση.

Ως εκ τούτου, η πρόταση ευθυγραμμίζεται άμεσα με την πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων, η οποία αποσκοπεί στην ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων έναντι υλικών απειλών σε μεγάλο αριθμό τομέων.

[1] COM(2020) 605 final.

Η πρόταση έχει ως στόχο να διασφαλίσει ότι, δυνάμει αμφότερων των νομικών πράξεων, οι αρμόδιες αρχές λαμβάνουν συμπληρωματικά μέτρα και ανταλλάσσουν πληροφορίες — ανάλογα με τις ανάγκες— όσον αφορά την ανθεκτικότητα εντός και εκτός κυβερνοχώρου, και ότι οι ιδιαίτερα κρίσιμοι φορείς εκμετάλλευσης στους τομείς που θεωρούνται «βασικοί» κατά την παρούσα πρόταση υπέχουν επίσης γενικότερες υποχρεώσεις ενίσχυσης της ανθεκτικότητας, με έμφαση στους κινδύνους που δεν σχετίζονται με τον κυβερνοχώρο.

- **Συνέπεια με άλλες πολιτικές της Ένωσης**

Όπως ορίζεται στην ανακοίνωση της Επιτροπής με τίτλο «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης»[2], η Ευρώπη είναι κρίσιμο να αξιοποιήσει όλα τα οφέλη της ψηφιακής εποχής και να ενισχύσει τη βιομηχανική ικανότητά της και την ικανότητά της για καινοτομία, εντός ασφαλών και δεοντολογικών ορίων. Η ευρωπαϊκή στρατηγική για τα δεδομένα καθορίζει τέσσερις πυλώνες —προστασία δεδομένων, θεμελιώδη δικαιώματα, ασφάλεια και κυβερνοασφάλεια— ως βασικές προϋποθέσεις για μια κοινωνία που βασίζεται στη χρήση δεδομένων.

Σε ψήφισμά του της 12ης Μαρτίου 2019, το Ευρωπαϊκό Κοινοβούλιο κάλεσε *«[...] την Επιτροπή να αξιολογήσει την ανάγκη περαιτέρω διεύρυνσης του πεδίου εφαρμογής της οδηγίας NIS σε άλλους κρίσιμους τομείς και υπηρεσίες που δεν καλύπτονται από ειδική τομεακή νομοθεσία»*[3]. Το Συμβούλιο, στα συμπεράσματά του της 9ης Ιουνίου 2020, επικρότησε *«[...] τα σχέδια της Επιτροπής να διασφαλίσει συνεπείς κανόνες για τους φορείς της αγοράς και να διευκολύνει την ασφαλή, αξιόπιστη και κατάλληλη ανταλλαγή πληροφοριών σχετικά με απειλές και συμβάντα, μεταξύ άλλων μέσω της αναθεώρησης της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (οδηγία NIS), να επιδιώξει λύσεις για τη βελτίωση της ανθεκτικότητας στον κυβερνοχώρο και την αποτελεσματικότερη αντιμετώπιση των επιθέσεων στον κυβερνοχώρο, ιδίως όσον αφορά βασικές οικονομικές και κοινωνικές δραστηριότητες, με παράλληλο σεβασμό των αρμοδιοτήτων των κρατών μελών, συμπεριλαμβανομένης της ευθύνης για την εθνική τους ασφάλεια»*[4]. Επιπλέον, η προτεινόμενη νομική πράξη δεν θίγει την εφαρμογή των κανόνων ανταγωνισμού που προβλέπονται στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

Δεδομένου ότι σημαντικό μέρος των απειλών για την κυβερνοασφάλεια προέρχονται από χώρες εκτός ΕΕ, είναι αναγκαία μια συνεκτική προσέγγιση της διεθνούς συνεργασίας. Η παρούσα οδηγία αποτελεί πρότυπο αναφοράς που πρέπει να προωθηθεί στο πλαίσιο της συνεργασίας της ΕΕ με τρίτες χώρες, ιδίως κατά την παροχή εξωτερικής τεχνικής βοήθειας.

2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

- **Νομική βάση**

Νομική βάση της οδηγίας NIS είναι το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων σχετικά με την προσέγγιση των εθνικών κανόνων. Όπως έκρινε το Δικαστήριο της ΕΕ στην απόφασή του στην υπόθεση C-58/08 Vodafone κ.λπ., η επίκληση του άρθρου 114 της ΣΛΕΕ δικαιολογείται όταν υπάρχουν

[2] COM(2020) 67 final.

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EL.html

[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/el/pdf

διαφορές μεταξύ εθνικών ρυθμίσεων που έχουν άμεση επίπτωση στη λειτουργία της εσωτερικής αγοράς. Ομοίως, το Δικαστήριο έκρινε ότι όταν μια στηριζόμενη στο άρθρο 114 της ΣΛΕΕ ρύθμιση έχει ήδη εξαλείψει κάθε εμπόδιο στο εμπόριο στον τομέα που εναρμονίζει, ο ενωσιακός νομοθέτης δεν στερείται της δυνατότητας προσαρμογής της εν λόγω ρύθμισης σε κάθε μεταβολή των περιστάσεων ή σε κάθε εξέλιξη των γνώσεων δεδομένου του καθήκοντος που τον βαρύνει σχετικά με την προστασία των γενικών συμφερόντων που αναγνωρίζει η Συνθήκη. Τέλος, το Δικαστήριο έκρινε ότι τα μέτρα σχετικά με την προσέγγιση που εμπίπτουν στο πεδίο εφαρμογής του άρθρου 114 της ΣΛΕΕ αποσκοπούν στο να απονείμουν στον νομοθέτη, σε συνάρτηση με το γενικό πλαίσιο και τις ειδικές περιστάσεις τού υπό εναρμόνιση τομέα, ορισμένη διακριτική ευχέρεια ως προς το ποια είναι η πιο ενδεδειγμένη μέθοδος προσέγγισης για την επίτευξη του επιδιωκόμενου αποτελέσματος. Η προτεινόμενη νομική πράξη θα άρει τα εμπόδια και θα βελτιώσει την εγκαθίδρυση και τη λειτουργία της εσωτερικής αγοράς για βασικές και σημαντικές οντότητες, θεσπίζοντας σαφείς κανόνες γενικής εφαρμογής σχετικά με το πεδίο εφαρμογής της οδηγίας NIS και εναρμονίζοντας τους κανόνες που εφαρμόζονται στον τομέα της διαχείρισης κινδύνων κυβερνοασφάλειας και της αναφοράς περιστατικών. Οι υφιστάμενες διαφορές στον τομέα αυτό, τόσο σε νομοθετικό όσο και σε εποπτικό επίπεδο, καθώς και σε εθνικό και ενωσιακό επίπεδο, αποτελούν εμπόδια για την εσωτερική αγορά, διότι οι οντότητες που ασκούν διασυνοριακές δραστηριότητες αντιμετωπίζουν διαφορετικές, και ενδεχομένως αλληλεπικαλυπτόμενες, κανονιστικές απαιτήσεις και/ή διαφορετική ή αλληλεπικαλυπτόμενη εφαρμογή αυτών των απαιτήσεων, εις βάρος της άσκησης των ελευθεριών τους όσον αφορά την εγκατάσταση και την παροχή υπηρεσιών. Η διαφορά μεταξύ των κανόνων έχει επίσης αρνητικό αντίκτυπο στις συνθήκες ανταγωνισμού στην εσωτερική αγορά, όταν πρόκειται για οντότητες του ίδιου τύπου σε διαφορετικά κράτη μέλη.

- **Επικουρικότητα (σε περίπτωση μη αποκλειστικής αρμοδιότητας)**

Η ανθεκτικότητα της κυβερνοασφάλειας σε ολόκληρη την Ένωση δεν μπορεί να είναι αποτελεσματική αν ακολουθείται ανομοιογενής προσέγγιση με εθνικά ή περιφερειακά στεγανά. Η οδηγία NIS κάλυψε εν μέρει αυτήν την αδυναμία, καθορίζοντας ένα πλαίσιο για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων σε εθνικό και ενωσιακό επίπεδο. Ωστόσο, η μεταφορά και η εφαρμογή της αποκάλυψαν επίσης εγγενείς αδυναμίες και περιορισμούς ορισμένων διατάξεων ή προσεγγίσεων, όπως η ασαφής οριοθέτηση του πεδίου εφαρμογής της οδηγίας, με αποτέλεσμα να υπάρχουν σημαντικές διαφορές ως προς την έκταση και το βάθος της de facto παρέμβασης της ΕΕ σε επίπεδο κρατών μελών. Επιπλέον, μετά την κρίση της COVID-19, η εξάρτηση της ευρωπαϊκής οικονομίας από δικτυακά και πληροφοριακά συστήματα έγινε μεγαλύτερη από ποτέ, ενώ οι τομείς και οι υπηρεσίες είναι ολοένα και πιο διασυνδεδεμένοι. Η παρέμβαση της ΕΕ που υπερβαίνει τα ισχύοντα μέτρα της οδηγίας NIS δικαιολογείται κυρίως από: i) τον ολοένα και πιο διασυνοριακό χαρακτήρα των απειλών και των προκλήσεων που σχετίζονται με την τα δικτυακά και πληροφοριακά συστήματα, ii) τις δυνατότητες της δράσης της ΕΕ για τη βελτίωση και τη διευκόλυνση αποτελεσματικών και συντονισμένων εθνικών πολιτικών, και iii) τη συμβολή συντονισμένων και συνεργατικών δράσεων πολιτικής στην αποτελεσματική προστασία των δεδομένων και της ιδιωτικής ζωής.

- **Αναλογικότητα**

Οι κανόνες που προτείνονται στην παρούσα οδηγία δεν υπερβαίνουν τα αναγκαία για την ικανοποιητική επίτευξη των ειδικών στόχων. Η προβλεπόμενη ευθυγράμμιση και ο προβλεπόμενος εξορθολογισμός των μέτρων ασφάλειας και των υποχρεώσεων αναφοράς

περιστατικών σχετίζονται με τα αιτήματα των κρατών μελών και των επιχειρήσεων για βελτίωση του ισχύοντος πλαισίου.

Η πρόταση λαμβάνει υπόψη τις ήδη υφιστάμενες πρακτικές στα κράτη μέλη. Το ενισχυμένο επίπεδο προστασίας που επιτυγχάνεται μέσω αυτών των εξορθολογισμένων και συντονισμένων απαιτήσεων είναι ανάλογο προς τους ολοένα και μεγαλύτερους κινδύνους που ανακύπτουν, συμπεριλαμβανομένων εκείνων που χαρακτηρίζονται από διασυνοριακά στοιχεία. Οι απαιτήσεις είναι εύλογες και ανταποκρίνονται γενικά στο συμφέρον των εμπλεκόμενων οντοτήτων για διασφάλιση της συνέχειας και της ποιότητας των υπηρεσιών τους. Το κόστος διασφάλισης της συστηματικής συνεργασίας μεταξύ των κρατών μελών θα είναι μικρό σε σύγκριση με τις οικονομικές και κοινωνικές απώλειες και ζημίες που προκαλούν τα περιστατικά κυβερνοασφάλειας. Επιπλέον, από τις διαβουλεύσεις με τα ενδιαφερόμενα μέρη που πραγματοποιήθηκαν στο πλαίσιο της αναθεώρησης της οδηγίας NIS, συμπεριλαμβανομένων των αποτελεσμάτων της ανοικτής δημόσιας διαβούλευσης και των στοχευμένων ερευνών, προκύπτει ότι υπάρχει υποστήριξη για την αναθεώρηση της οδηγίας NIS σύμφωνα με τις προαναφερθείσες κατευθυντήριες γραμμές.

- **Επιλογή της νομικής πράξης**

Η πρόταση θα εξορθολογίσει περαιτέρω τις υποχρεώσεις που επιβάλλονται στις επιχειρήσεις και θα αυξήσει το επίπεδο εναρμόνισής τους. Ταυτοχρόνως, η πρόταση έχει ως στόχο να παράσχει στα κράτη μέλη την απαιτούμενη ευελιξία ώστε να λαμβάνουν υπόψη τις εθνικές ιδιαιτερότητες (όπως η δυνατότητα εντοπισμού πρόσθετων βασικών ή σημαντικών οντοτήτων που υπερβαίνουν το βασικό σενάριο που καθορίζεται στη νομική πράξη). Ως εκ τούτου, το μελλοντικό νομικό μέσο θα πρέπει να είναι οδηγία, δεδομένου αυτός ο νομικός τύπος επιτρέπει τη στοχευμένη βελτίωση της εναρμόνισης, αλλά και έναν ορισμένο βαθμό ευελιξίας για τις αρμόδιες αρχές.

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

- **Εκ των υστέρων αξιολογήσεις / έλεγχοι καταλληλότητας της ισχύουσας νομοθεσίας**

Η Επιτροπή προέβη σε αξιολόγηση της λειτουργίας της οδηγίας NIS[5]. Ανέλυσε τη συνάφεια, την ενωσιακή προστιθέμενη αξία, τη συνοχή, την αποτελεσματικότητα και την αποδοτικότητά της. Τα κυριότερα συμπεράσματα της ανάλυσης έχουν ως εξής:

- Το πεδίο εφαρμογής της οδηγίας NIS είναι υπερβολικά περιορισμένο όσον αφορά τους τομείς που καλύπτει, κυρίως λόγω i) της αυξημένης ψηφιοποίησης κατά τα τελευταία έτη και του υψηλότερου βαθμού διασύνδεσης, και ii) του πεδίου εφαρμογής της οδηγίας NIS, το οποίο δεν καλύπτει πλέον όλους τους ψηφιοποιημένους τομείς που παρέχουν βασικές υπηρεσίες στην οικονομία και την κοινωνία στο σύνολό της.
- Η οδηγία NIS δεν είναι επαρκώς σαφής όσον αφορά το πεδίο εφαρμογής για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και οι διατάξεις της δεν παρέχουν επαρκή σαφήνεια όσον αφορά την εθνική αρμοδιότητα επί των παρόχων ψηφιακών υπηρεσιών. Αυτό οδήγησε σε μια κατάσταση στην οποία ορισμένα είδη οντοτήτων

[5] [Παράρτημα 5 της εκτίμησης επιπτώσεων]

δεν έχουν προσδιοριστεί σε όλα τα κράτη μέλη και, ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν μέτρα ασφάλειας και να αναφέρουν περιστατικά.

- Η οδηγία NIS παρείχε ευρεία διακριτική ευχέρεια στα κράτη μέλη κατά τον καθορισμό απαιτήσεων όσον αφορά την ασφάλεια και την αναφορά περιστατικών για τους φορείς εκμετάλλευσης βασικών υπηρεσιών. Από την αξιολόγηση προκύπτει ότι, σε ορισμένες περιπτώσεις, τα κράτη μέλη έχουν εφαρμόσει τις απαιτήσεις αυτές με πολύ διαφορετικούς τρόπους, γεγονός που δημιουργεί πρόσθετη επιβάρυνση για τις εταιρείες που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη.
- Το καθεστώς εποπτείας και επιβολής της οδηγίας NIS είναι αναποτελεσματικό. Για παράδειγμα, τα κράτη μέλη ήταν πολύ απρόθυμα να επιβάλουν κυρώσεις σε οντότητες που δεν έχουν θεσπίσει απαιτήσεις ασφάλειας ή δεν αναφέρουν περιστατικά. Αυτό μπορεί να έχει αρνητικές συνέπειες για την κυβερνοανθεκτικότητα μεμονωμένων οντοτήτων.
- Οι οικονομικοί και ανθρώπινοι πόροι που διαθέτουν τα κράτη μέλη για την εκπλήρωση των καθηκόντων τους (όπως ο προσδιορισμός ή η εποπτεία των φορέων εκμετάλλευσης βασικών υπηρεσιών) και, κατά συνέπεια, τα διαφορετικά επίπεδα ωριμότητας όσον αφορά την αντιμετώπιση των κινδύνων κυβερνοασφάλειας, ποικίλλουν σε μεγάλο βαθμό. Αυτό εντείνει περαιτέρω τις διαφορές όσον αφορά την κυβερνοανθεκτικότητα μεταξύ των κρατών μελών.
- Τα κράτη μέλη δεν ανταλλάσσουν συστηματικά πληροφορίες μεταξύ τους, γεγονός που έχει αρνητικές συνέπειες ιδίως για την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας και για το επίπεδο κοινής επίγνωσης της κατάστασης στο σύνολο της ΕΕ. Το ίδιο ισχύει και για την ανταλλαγή πληροφοριών μεταξύ ιδιωτικών οντοτήτων, αλλά και για τη συνεργασία μεταξύ των δομών συνεργασίας σε επίπεδο ΕΕ και των ιδιωτικών οντοτήτων.
- **Διαβουλεύσεις με τα ενδιαφερόμενα μέρη**

Η Επιτροπή έχει προβεί σε διαβουλεύσεις με ένα ευρύ φάσμα ενδιαφερομένων μερών. Τα κράτη μέλη και τα ενδιαφερόμενα μέρη κλήθηκαν να συμμετάσχουν στην ανοικτή δημόσια διαβούλευση, καθώς και στις έρευνες και τα εργαστήρια που διοργάνωσαν οι Wavestone, CEPS και ICF, στις οποίες η Επιτροπή έχει αναθέσει τη διεξαγωγή μελέτης για την υποστήριξη της αναθεώρησης της οδηγίας NIS. Τα ενδιαφερόμενα μέρη που συμμετείχαν στις διαβουλεύσεις ήταν αρμόδιες αρχές, όργανα της Ένωσης που ασχολούνται με την κυβερνοασφάλεια, φορείς εκμετάλλευσης βασικών υπηρεσιών, πάροχοι ψηφιακών υπηρεσιών, οντότητες που παρέχουν υπηρεσίες εκτός του πεδίου εφαρμογής της ισχύουσας οδηγίας NIS, εμπορικές ενώσεις και οργανώσεις καταναλωτών, καθώς και πολίτες.

Επιπλέον, η Επιτροπή βρίσκεται σε συνεχή επαφή με τις αρμόδιες αρχές που είναι επιφορτισμένες με την εφαρμογή της οδηγίας NIS. Η ομάδα συνεργασίας έχει καλύψει εκτενώς διάφορες οριζόντιες και τομεακές πτυχές εφαρμογής. Τέλος, κατά τις επισκέψεις της στα κράτη μέλη με θέμα την οδηγία NIS, το 2019 και το 2020, η Επιτροπή πραγματοποίησε συνεντεύξεις με 154 δημόσιους και ιδιωτικούς φορείς, καθώς και με 117 αρμόδιες αρχές.

- **Συλλογή και χρήση εμπειρογνωσίας**

Η Επιτροπή έχει αναθέσει σε κοινοπραξία των Wavestone, CEPS και ICF να την υποστηρίξει στην αναθεώρηση της οδηγίας NIS[6]. Η ανάδοχος δεν έχει έρθει μόνο σε επαφή με τα ενδιαφερόμενα μέρη που επηρεάζονται άμεσα από την οδηγία NIS, μέσω στοχευμένων ερευνών και εργαστηρίων, αλλά έχει διαβουλευθεί και με ευρύ φάσμα εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας, π.χ. με ερευνητές στον τομέα της κυβερνοασφάλειας και με επαγγελματίες του κλάδου της κυβερνοασφάλειας.

- **Εκτίμηση επιπτώσεων**

Η παρούσα πρόταση συνοδεύεται από εκτίμηση επιπτώσεων[7], η οποία υποβλήθηκε στην επιτροπή ρυθμιστικού ελέγχου (στο εξής: ΕΡΕ) στις 23 Οκτωβρίου 2020 και έλαβε θετική γνώμη με παρατηρήσεις από την ΕΡΕ στις 20 Νοεμβρίου 2020. Η ΕΡΕ συνέστησε βελτιώσεις σε ορισμένους τομείς με σκοπό: 1) να αποτυπωθεί καλύτερα ο ρόλος των διασυνοριακών δευτερογενών επιπτώσεων στην ανάλυση του προβλήματος, 2) να εξηγηθεί καλύτερα το τι θα συνιστά επιτυχία για την πρωτοβουλία, 3) να αιτιολογηθεί περαιτέρω ο κατάλογος των επιλογών πολιτικής, 4) να αναλυθεί περαιτέρω το κόστος των προτεινόμενων μέτρων. Η εκτίμηση επιπτώσεων προσαρμόστηκε με γνώμονα αυτά τα σημεία, καθώς και με λεπτομερέστερες παρατηρήσεις της ΕΡΕ. Πλέον περιλαμβάνει αναλυτικότερες εξηγήσεις σχετικά με τον ρόλο των διασυνοριακών δευτερογενών επιπτώσεων στον τομέα της κυβερνοασφάλειας, σαφέστερη επισκόπηση του τρόπου μέτρησης της επιτυχίας, λεπτομερέστερη επεξήγηση του σχεδιασμού και της λογικής πίσω από τις διάφορες επιλογές πολιτικής και τις δράσεις που εξετάζονται στο πλαίσιο αυτών των επιλογών, λεπτομερέστερη επεξήγηση των πτυχών που αναλύονται όσον αφορά το τομεακό πεδίο εφαρμογής της οδηγίας NIS, καθώς και περαιτέρω διευκρινίσεις σχετικά με το κόστος.

Η Επιτροπή εξέτασε μια σειρά επιλογών πολιτικής για τη βελτίωση του νομικού πλαισίου στον τομέα της κυβερνοανθεκτικότητας και της αντιμετώπισης περιστατικών:

- «Μη ανάληψη δράσης»: Η οδηγία NIS θα παραμείνει αμετάβλητη και δεν θα ληφθούν άλλα μέτρα μη νομοθετικού χαρακτήρα για την αντιμετώπιση των προβλημάτων που εντοπίστηκαν κατά την αξιολόγηση της οδηγίας NIS.
- Επιλογή 1: Δεν θα υπάρξουν αλλαγές σε νομοθετικό επίπεδο. Αντ' αυτού, η Επιτροπή θα εκδώσει συστάσεις και κατευθυντήριες γραμμές (π.χ. για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών, τις απαιτήσεις ασφάλειας, τις διαδικασίες κοινοποίησης περιστατικών και την εποπτεία), κατόπιν διαβούλευσης με την ομάδα συνεργασίας, τον Οργανισμό της ΕΕ για την Κυβερνοασφάλεια (ENISA) και, κατά περίπτωση, με το δίκτυο των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT).
- Επιλογή 2: Η επιλογή αυτή περιλαμβάνει στοχευμένες τροποποιήσεις της οδηγίας NIS, συμπεριλαμβανομένης της επέκτασης του πεδίου εφαρμογής της και πολλών άλλων τροποποιήσεων που θα αποσκοπούν στην εξασφάλιση ορισμένων άμεσων λύσεων στα προβλήματα που έχουν εντοπιστεί, καθώς και στην παροχή σαφήνειας

6 Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665 [μελέτη για την υποστήριξη της αναθεώρησης της οδηγίας (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (οδηγία NIS) – αριθ. 2020-665]. Wavestone, CEPS και ICF.

7 **[Links to final document and to the summary sheet to be added.]**

και περαιτέρω εναρμόνισης (π.χ. διατάξεις για την εναρμόνιση των ορίων προσδιορισμού). Ωστόσο, η τροποποιημένη οδηγία NIS θα διατηρήσει τα ίδια κύρια δομικά στοιχεία, προσέγγιση και σκεπτικό.

- Επιλογή 3: Το σενάριο αυτό προβλέπει συστημικές και διαρθρωτικές αλλαγές στην οδηγία NIS (μέσω νέας οδηγίας) οι οποίες προβλέπουν μια πιο θεμελιώδη στροφή της προσέγγισης προς την κάλυψη ενός ευρύτερου τμήματος των οικονομιών σε ολόκληρη την Ένωση, αλλά με πιο εστιασμένη εποπτεία που θα επικεντρώνεται στους μεγάλους και βασικούς παίκτες. Επίσης, θα εξορθολογίσει τις υποχρεώσεις που επιβάλλονται στις επιχειρήσεις και θα εξασφαλίσει ένα υψηλότερο επίπεδο εναρμόνισής τους, θα δημιουργήσει ένα πιο αποτελεσματικό πλαίσιο για τις επιχειρησιακές πτυχές, και θα θέσει μια σαφή βάση για ενισχυμένες κοινές ευθύνες και λογοδοσία των διαφόρων ενδιαφερόμενων μερών όσον αφορά τα μέτρα για την κυβερνοασφάλεια.

Από την εκτίμηση επιπτώσεων συνάγεται το συμπέρασμα ότι προτιμώμενη επιλογή είναι η επιλογή 3 (δηλαδή οι συστημικές και διαρθρωτικές αλλαγές του πλαισίου της οδηγίας NIS). Όσον αφορά την αποτελεσματικότητα, η προτιμώμενη επιλογή θα ορίσει σαφώς το πεδίο εφαρμογής της οδηγίας NIS —το οποίο θα επεκταθεί σε ένα πιο αντιπροσωπευτικό τμήμα των οικονομιών και των κοινωνιών της ΕΕ— και τον εξορθολογισμό των απαιτήσεων, μαζί με ένα πιο καθορισμένο πλαίσιο εποπτείας και επιβολής που θα αποσκοπεί στην αύξηση του επιπέδου συμμόρφωσης. Επίσης, περιλαμβάνει μέτρα που αποσκοπούν στη βελτίωση των προσεγγίσεων χάραξης πολιτικής σε επίπεδο κρατών μελών και στην αλλαγή του προτύπου τους, με την προώθηση νέων πλαισίων για τη διαχείριση κινδύνου στις σχέσεις με τους προμηθευτές και για τη συντονισμένη γνωστοποίηση τρωτών σημείων. Ταυτοχρόνως, η προτιμώμενη επιλογή πολιτικής θεσπίζει μια σαφή βάση για τις κοινές ευθύνες και τη λογοδοσία και προβλέπει μηχανισμούς που αποσκοπούν στην ενίσχυση της εμπιστοσύνης μεταξύ των κρατών μελών, τόσο των αρχών όσο και του κλάδου, παρέχοντας κίνητρα για την ανταλλαγή πληροφοριών και προάγοντας μια πιο επιχειρησιακή προσέγγιση, π.χ. μέσω αμοιβαίας συνδρομής και μηχανισμών αξιολόγησης από ομοτίμους. Η επιλογή αυτή θα προβλέπει επίσης ένα ενωσιακό πλαίσιο διαχείρισης κρίσεων, με βάση το επιχειρησιακό δίκτυο της ΕΕ που δρομολογήθηκε πρόσφατα, και θα εξασφαλίσει μεγαλύτερη συμμετοχή του ENISA, στο πλαίσιο της τρέχουσας εντολής του, όσον αφορά την ακριβή επισκόπηση της κατάστασης της κυβερνοασφάλειας στην Ένωση.

Όσον αφορά την αποδοτικότητα, η προτιμώμενη επιλογή θα επιφέρει μεν πρόσθετο κόστος συμμόρφωσης και επιβολής για τις επιχειρήσεις και τα κράτη μέλη, αλλά θα οδηγήσει και σε αποδοτικές αντισταθμίσεις και συνέργειες, με τις βέλτιστες δυνατότητες από όλες τις επιλογές πολιτικής που αναλύθηκαν, ώστε να διασφαλιστεί ένα αυξημένο και συνεκτικό επίπεδο κυβερνοανθεκτικότητας των βασικών οντοτήτων σε ολόκληρη την Ένωση, το οποίο θα οδηγήσει εν τέλει σε εξοικονόμηση κόστους τόσο για τις επιχειρήσεις όσο και για την κοινωνία. Αυτή η επιλογή πολιτικής θα επιφέρει ορισμένο πρόσθετο διοικητικό φόρτο και κόστος συμμόρφωσης για τις αρχές των κρατών μελών. Ωστόσο, σε τελική ανάλυση, μεσοπρόθεσμα και μακροπρόθεσμα, θα αποφέρει επίσης σημαντικά οφέλη με την αυξημένη συνεργασία μεταξύ των κρατών μελών, μεταξύ άλλων και σε επιχειρησιακό επίπεδο, αλλά και με την παροχή κινήτρων —μέσω της αμοιβαίας συνδρομής, των μηχανισμών αξιολόγησης από ομοτίμους, και της καλύτερης εποπτείας και αλληλεπίδρασης με τις βασικές επιχειρήσεις— για μια συνολική αύξηση των ικανοτήτων κυβερνοασφάλειας σε εθνικό και περιφερειακό επίπεδο. Η προτιμώμενη επιλογή πολιτικής θα διασφαλίσει επίσης σε μεγάλο βαθμό τη συνοχή με άλλες νομοθετικές πράξεις, πρωτοβουλίες ή μέτρα πολιτικής, συμπεριλαμβανομένου του lex specialis που άπτεται του τομέα.

Η αντιμετώπιση της τρέχουσας ανεπάρκειας όσον αφορά την ετοιμότητα στον τομέα της κυβερνοασφάλειας σε επίπεδο κρατών μελών και σε επίπεδο εταιρειών και άλλων οργανισμών θα μπορούσε να αποφέρει αύξηση της αποδοτικότητας και μείωση του πρόσθετου κόστους που προκύπτει από περιστατικά κυβερνοασφάλειας.

- Για τις βασικές και σημαντικές οντότητες, η αύξηση του επιπέδου ετοιμότητας στον τομέα της κυβερνοασφάλειας θα μπορούσε να έχει ως αποτέλεσμα τον μετριασμό της πιθανής απώλειας εσόδων λόγω διαταραχών —π.χ. λόγω βιομηχανικής κατασκοπείας— και θα μπορούσε να μειώσει τις μεγάλες δαπάνες του ad hoc μετριασμού των απειλών. Αυτές οι ωφέλειες πιθανότατα υπερκαλύπτουν το επενδυτικό κόστος που απαιτείται. Επίσης, η μείωση του κατακερματισμού στην εσωτερική αγορά θα βελτιώσει την ισοτιμία των όρων του ανταγωνισμού μεταξύ των φορέων εκμετάλλευσης.
- Για τα κράτη μέλη, θα μπορούσε να μειώσει περαιτέρω τον κίνδυνο αύξησης των δημοσιονομικών δαπανών για τον ad hoc μετριασμό των απειλών και των πρόσθετων δαπανών σε περιπτώσεις έκτακτης ανάγκης που σχετίζονται με περιστατικά κυβερνοασφάλειας.
- Για τους πολίτες, η αντιμετώπιση των περιστατικών κυβερνοασφάλειας αναμένεται να αποφέρει μείωση της απώλειας εισοδήματος εξαιτίας οικονομικών διαταραχών.

Τα αυξημένα επίπεδα κυβερνοασφάλειας στο σύνολο των κρατών μελών και η ικανότητα των εταιρειών και των αρχών να αντιδρούν γρήγορα σε περιστατικά και να μετριάζουν τον αντίκτυπό τους θα έχουν πιθανότατα ως αποτέλεσμα την αύξηση της συνολικής εμπιστοσύνης των πολιτών στην ψηφιακή οικονομία, γεγονός που θα μπορούσε να έχει θετικό αντίκτυπο στην ανάπτυξη και τις επενδύσεις.

Η αύξηση του συνολικού επιπέδου κυβερνοασφάλειας είναι πιθανό να οδηγήσει στην αύξηση της συνολικής ασφάλειας και στην ομαλή αδιάλειπτη λειτουργία των βασικών υπηρεσιών, οι οποίες είναι κρίσιμες για την κοινωνία. Η πρωτοβουλία μπορεί επίσης να συμβάλει στην επίτευξη και άλλων κοινωνικών αποτελεσμάτων, όπως η μείωση των επιπέδων κυβερνοεγκλήματος και τρομοκρατίας και η αύξηση της πολιτικής προστασίας. Η αύξηση του επιπέδου κυβερνοετοιμότητας των επιχειρήσεων και άλλων οργανισμών μπορεί να αποτρέψει πιθανές οικονομικές απώλειες εξαιτίας κυβερνοεπιθέσεων, προλαμβάνοντας έτσι την ανάγκη απόλυσης εργαζομένων.

Η αύξηση του συνολικού επιπέδου κυβερνοασφάλειας θα μπορούσε επίσης να οδηγήσει στην πρόληψη περιβαλλοντικών κινδύνων/ζημιών σε περίπτωση επίθεσης σε βασική υπηρεσία. Αυτό μπορεί να ισχύει ιδιαίτερα για τους τομείς της ενέργειας, της παροχής και διανομής νερού ή των μεταφορών. Με την ενίσχυση των ικανοτήτων κυβερνοασφάλειας, η πρωτοβουλία θα μπορούσε να οδηγήσει στην αύξηση της χρήσης των υποδομών και υπηρεσιών ΤΠΕ τελευταίας γενιάς, που είναι και πιο βιώσιμες από περιβαλλοντική άποψη, καθώς και στην αντικατάσταση αναποτελεσματικών και λιγότερο ασφαλών υποδομών παλαιού τύπου. Αυτό αναμένεται να συμβάλει και στη μείωση του αριθμού των δαπανηρών περιστατικών κυβερνοασφάλειας, απελευθερώνοντας πόρους για βιώσιμες επενδύσεις.

- **Καταλληλότητα και απλούστευση του κανονιστικού πλαισίου**

Η πρόταση προβλέπει γενική εξαίρεση των πολύ μικρών και μικρών οντοτήτων από το πεδίο εφαρμογής της οδηγίας NIS και ένα λιγότερο αυστηρό καθεστώς εκ των υστέρων εποπτείας για μεγάλο αριθμό νέων οντοτήτων που εμπίπτουν στο αναθεωρημένο πεδίο εφαρμογής (τις λεγόμενες «σημαντικές οντότητες»). Τα μέτρα αυτά αποσκοπούν στην ελαχιστοποίηση και

την εξισορρόπηση του φόρτου που βαρύνει τις εταιρείες και τις δημόσιες διοικήσεις. Επιπλέον, η πρόταση αντικαθιστά το πολύπλοκο σύστημα προσδιορισμού των φορέων εκμετάλλευσης βασικών υπηρεσιών με μια υποχρέωση γενικής εφαρμογής, και θεσπίζει υψηλότερο επίπεδο εναρμόνισης των υποχρεώσεων ασφάλειας και αναφοράς περιστατικών, γεγονός που θα μειώσει τον φόρτο συμμόρφωσης, ιδίως για τις οντότητες που παρέχουν διασυνοριακές υπηρεσίες.

Η πρόταση ελαχιστοποιεί το κόστος συμμόρφωσης για τις ΜΜΕ, δεδομένου ότι οι οντότητες υποχρεούνται να λαμβάνουν μόνο τα μέτρα που είναι αναγκαία για τη διασφάλιση ενός επιπέδου ασφάλειας των δικτυακών και πληροφοριακών συστημάτων που είναι ανάλογο με τον εκάστοτε κίνδυνο.

- **Θεμελιώδη δικαιώματα**

Η ΕΕ είναι προσηλωμένη στη διασφάλιση υψηλών προτύπων προστασίας των θεμελιωδών δικαιωμάτων. Όλες οι ρυθμίσεις εθελούσιας ανταλλαγής πληροφοριών μεταξύ οντοτήτων τις οποίες προάγει η παρούσα οδηγία θα διεξάγονται σε περιβάλλοντα εμπιστοσύνης, με πλήρη σεβασμό των κανόνων της Ένωσης για την προστασία των δεδομένων, και ιδίως του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[8].

4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Βλ. δημοσιονομικό δελτίο

5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

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

Η πρόταση περιλαμβάνει ένα γενικό σχέδιο για την παρακολούθηση και την αξιολόγηση των επιπτώσεων στους ειδικούς στόχους, βάσει του οποίου η Επιτροπή υποχρεούται να προβεί σε επανεξέταση τουλάχιστον [54 μήνες] μετά την έναρξη ισχύος και να υποβάλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με τα κύρια πορίσματά της.

Η επανεξέταση πρέπει να διενεργηθεί σύμφωνα με τις κατευθυντήριες γραμμές της Επιτροπής για τη βελτίωση της νομοθεσίας.

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

Η πρόταση διαρθρώνεται γύρω από διάφορους βασικούς τομείς πολιτικής, οι οποίοι είναι αλληλένδετοι και εξυπηρετούν τον σκοπό της αύξησης του επιπέδου κυβερνοασφάλειας στην Ένωση.

Αντικείμενο και πεδίο εφαρμογής (άρθρα 1 και 2)

Η οδηγία, ειδικότερα: α) θεσπίζει υποχρεώσεις για τα κράτη μέλη όσον αφορά τη θέσπιση εθνικής στρατηγικής κυβερνοασφάλειας και τον ορισμό αρμόδιων εθνικών αρχών, ενιαίων σημείων επαφής, και CSIRT, β) προβλέπει ότι τα κράτη μέλη θα θεσπίσουν υποχρεώσεις διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας για τις

[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).

οντότητες που αναφέρονται ως βασικές οντότητες στο παράρτημα I και ως σημαντικές οντότητες στο παράρτημα II, γ) προβλέπει ότι τα κράτη μέλη θα θεσπίσουν υποχρεώσεις σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια.

Εφαρμόζεται σε ορισμένες δημόσιες ή ιδιωτικές βασικές οντότητες που δραστηριοποιούνται στους τομείς που απαριθμούνται στο παράρτημα I (ενέργεια· μεταφορές· τράπεζες· υποδομές χρηματοπιστωτικών αγορών· υγεία, πόσιμο νερό· λύματα· ψηφιακές υποδομές· δημόσια διοίκηση και διάστημα) και σε ορισμένες σημαντικές οντότητες που δραστηριοποιούνται στους τομείς που απαριθμούνται στο παράρτημα II (ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών· διαχείριση αποβλήτων· παρασκευή, παραγωγή και διανομή χημικών προϊόντων· παραγωγή, μεταποίηση και διανομή τροφίμων· μεταποίηση και πάροχοι ψηφιακών υπηρεσιών). Οι πολύ μικρές και μικρές οντότητες, κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, εξαιρούνται από το πεδίο εφαρμογής της οδηγίας, πλην των παρόχων δικτύων ηλεκτρονικών επικοινωνιών ή των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, των παρόχων υπηρεσιών εμπιστοσύνης, των μητρώων ονομάτων τομέα ανωτάτου επιπέδου (στο εξής: TLD), και της δημόσιας διοίκησης, καθώς και ορισμένων άλλων οντοτήτων, όπως ο μοναδικός πάροχος υπηρεσίας σε κράτος μέλος.

Εθνικά πλαίσια κυβερνοασφάλειας (άρθρα 5 έως 11)

Τα κράτη μέλη οφείλουν να θεσπίσουν εθνική στρατηγική κυβερνοασφάλειας η οποία καθορίζει τους στρατηγικούς στόχους και κατάλληλα μέτρα πολιτικής και κανονιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας.

Η οδηγία θεσπίζει επίσης ένα πλαίσιο για τη συντονισμένη γνωστοποίηση τρωτών σημείων και απαιτεί από τα κράτη μέλη να ορίσουν CSIRT που θα ενεργούν ως αξιόπιστοι ενδιάμεσοι φορείς και θα διευκολύνουν την αλληλεπίδραση μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων και υπηρεσιών ΤΠΕ. Ο ENISA οφείλει να αναπτύξει και να τηρεί ευρωπαϊκό μητρώο τρωτών σημείων για τα τρωτά σημεία που εντοπίζονται.

Τα κράτη μέλη υποχρεούνται να θεσπίσουν εθνικά πλαίσια διαχείρισης κρίσεων κυβερνοασφάλειας, μεταξύ άλλων ορίζοντας εθνικές αρμόδιες αρχές υπεύθυνες για τη διαχείριση περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας.

Τα κράτη μέλη υποχρεούνται επίσης να ορίσουν μία ή περισσότερες εθνικές αρμόδιες αρχές κυβερνοασφάλειας για τα εποπτικά καθήκοντα που απορρέουν από την παρούσα οδηγία και ένα εθνικό ενιαίο σημείο επαφής για την κυβερνοασφάλεια (SPOC) που θα λειτουργεί ως σύνδεσμος για τη διασυνοριακή συνεργασία των αρχών των κρατών μελών. Τα κράτη μέλη υποχρεούνται επίσης να ορίσουν CSIRT.

Συνεργασία (άρθρα 12 έως 16)

Η οδηγία συστήνει ομάδα συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, καθώς και την ανάπτυξη της εμπιστοσύνης και της αξιοπιστίας μεταξύ τους. Επίσης, συστήνει δίκτυο CSIRT με σκοπό τη συμβολή στην ανάπτυξη της αξιοπιστίας και της εμπιστοσύνης μεταξύ των κρατών μελών και την προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας.

Συστήνεται ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe) με σκοπό τη στήριξη της συντονισμένης διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας και τη διασφάλιση της τακτικής ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και των θεσμικών οργάνων της ΕΕ.

Ο ENISA υποχρεούται να εκδίδει, σε συνεργασία με την Επιτροπή, έκθεση ανά διετία σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση.

Η Επιτροπή οφείλει να θεσπίσει ένα σύστημα αξιολόγησης από ομοτίμους που θα επιτρέπει την τακτική αξιολόγηση από ομοτίμους της αποτελεσματικότητας των πολιτικών κυβερνοασφάλειας των κρατών μελών.

Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις αναφοράς περιστατικών (άρθρα 17 έως 23)

Η οδηγία απαιτεί από τα κράτη μέλη να προβλέπουν ότι τα διοικητικά όργανα όλων των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας πρέπει να εγκρίνουν τα μέτρα διαχείρισης κινδύνου στον τομέα της κυβερνοασφάλειας που λαμβάνονται από τις οικείες οντότητες και να παρακολουθούν ειδική κατάρτιση σχετικά με την κυβερνοασφάλεια.

Τα κράτη μέλη οφείλουν να διασφαλίζουν ότι οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων κυβερνοασφάλειας, όσον αφορά την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων. Επίσης, οφείλουν να διασφαλίζουν ότι οι οντότητες κοινοποιούν στις αρμόδιες εθνικές αρχές ή στις CSIRT κάθε περιστατικό κυβερνοασφάλειας που έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που παρέχουν.

Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα στα μητρώα TLD θα συλλέγουν και θα τηρούν ακριβή και πλήρη δεδομένα καταχώρισης ονομάτων τομέα. Επιπλέον, οι εν λόγω οντότητες υποχρεούνται να παρέχουν αποτελεσματική πρόσβαση σε δεδομένα καταχώρισης τομέα στους νόμιμους αιτούντες πρόσβαση.

Δικαιοδοσία και καταχώριση (άρθρα 24 και 25)

Κατά κανόνα, οι βασικές και σημαντικές οντότητες θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. Ωστόσο, ορισμένα είδη οντοτήτων (πάροχοι υπηρεσιών DNS, μητρώα ονομάτων TLD, πάροχοι υπηρεσιών νεφοϋπολογιστικής, πάροχοι υπηρεσιών κέντρου δεδομένων και πάροχοι δικτύων διανομής περιεχομένου, καθώς και ορισμένοι πάροχοι ψηφιακών υπηρεσιών) θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση. Με τον τρόπο αυτό διασφαλίζεται ότι οι εν λόγω οντότητες δεν βαρύνονται με μια πληθώρα διαφορετικών νομικών απαιτήσεων, δεδομένου ότι παρέχουν, σε ιδιαίτερα υψηλό βαθμό, διασυνοριακές υπηρεσίες. Ο ENISA υποχρεούται να καταρτίσει και να τηρεί μητρώο αυτού του τελευταίου είδους οντοτήτων.

Ανταλλαγή πληροφοριών (άρθρα 26 και 27)

Τα κράτη μέλη θα θεσπίσουν κανόνες που επιτρέπουν στις οντότητες να συμμετέχουν στην ανταλλαγή πληροφοριών σχετικά με την κυβερνοασφάλεια, στο πλαίσιο ειδικών ρυθμίσεων για την ανταλλαγή πληροφοριών σχετικά με την κυβερνοασφάλεια, σύμφωνα με το άρθρο 101 της ΣΛΕΕ. Επιπλέον, τα κράτη μέλη θα επιτρέπουν σε οντότητες εκτός του πεδίου

εφαρμογής της παρούσας οδηγίας να αναφέρουν, σε εθελοντική βάση, σημαντικά περιστατικά, κυβερνοαπειλές, ή παρ᾽ ολίγον περιστατικά.

Εποπτεία και επιβολή (άρθρα 28 έως 34)

Οι αρμόδιες αρχές υποχρεούνται να εποπτεύουν τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας, και ιδίως να διασφαλίζουν τη συμμόρφωσή τους με τις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών. Η οδηγία διακρίνει μεταξύ ενός εκ των προτέρων εποπτικού καθεστώτος για τις βασικές οντότητες και ενός εκ των υστέρων εποπτικού καθεστώτος για τις σημαντικές οντότητες· εξ αυτών, το δεύτερο καθεστώς απαιτεί από τις αρμόδιες αρχές να αναλαμβάνουν δράση όταν λαμβάνουν αποδείξεις ή ενδείξεις ότι κάποια σημαντική οντότητα δεν πληροί τις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών.

Η οδηγία απαιτεί επίσης από τα κράτη μέλη να επιβάλλουν διοικητικά πρόστιμα σε βασικές και σημαντικές οντότητες και ορίζει ορισμένα μέγιστα πρόστιμα.

Τα κράτη μέλη υποχρεούνται να συνεργάζονται και να παρέχουν αμοιβαία συνδρομή, ανάλογα με τις ανάγκες, όταν οντότητες παρέχουν υπηρεσίες σε περισσότερα από ένα κράτη μέλη ή όταν η κύρια εγκατάσταση μιας οντότητας ή ο εκπρόσωπός της βρίσκεται σε κάποιο κράτος μέλος, αλλά τα δικτυακά και πληροφοριακά της συστήματα βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη.

2020/0359 (COD)

Πρόταση

ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

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

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Έχοντας υπόψη τη γνώμη της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής[9],

Έχοντας υπόψη τη γνώμη της Επιτροπής των Περιφερειών[10],

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Η οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11] αποσκοπούσε στην ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, στον μετριασμό των απειλών για τα δικτυακά και πληροφοριακά συστήματα που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών κυβερνοασφάλειας, ώστε να συμβάλει στην αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης.

(2) Αφότου άρχισε να ισχύει η οδηγία (ΕΕ) 2016/1148, έχει σημειωθεί σημαντική πρόοδος όσον αφορά την αύξηση του επιπέδου ανθεκτικότητας της κυβερνοασφάλειας 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 με τον καθορισμό εθνικών στρατηγικών κυβερνοασφάλειας, τη θέσπιση εθνικών ικανοτήτων και την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και φορείς που προσδιορίζονται από κάθε κράτος μέλος. Συνέβαλε επίσης στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας

[9] ΕΕ C της , σ. .

[10] ΕΕ C της , σ. .

[11] 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 194/1 της 19.7.2016, σ. 1).

συνεργασίας[12] και ενός δικτύου εθνικών ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών («δίκτυο CSIRT»)[13]. Παρά τα επιτεύγματα αυτά, η επανεξέταση της οδηγίας (ΕΕ) 2016/1148 αποκάλυψε εγγενείς αδυναμίες που την εμποδίζουν να αντιμετωπίσει αποτελεσματικά τις ταυτόχρονες και αναδυόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας.

(3) Τα δικτυακά και πληροφοριακά συστήματα 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 απειλών για την κυβερνοασφάλεια, 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 κυβερνοασφάλειας αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των δικτυακών και πληροφοριακών συστημάτων. Ως εκ τούτου, τα κυβερνοπεριστατικά μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων στην εσωτερική αγορά, να προκαλέσουν οικονομικές απώλειες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και των χρηστριών 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.

(4) Η νομική βάση της οδηγίας 1148/2016/ΕΕ 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 οικονομικά συναφείς δραστηριότητες ποικίλλουν σημαντικά μεταξύ των κρατών μελών ως προς το είδος της απαίτησης, τον βαθμό λεπτομερειακότητάς τους και τη μέθοδο εποπτείας. Οι διαφορές αυτές αυξάνουν το κόστος και προκαλούν δυσκολίες στις επιχειρήσεις 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 μη βέλτιστου σχεδιασμού ή εφαρμογής προτύπων κυβερνοασφάλειας σε ένα κράτος μέλος είναι πιθανό να επηρεάσει το επίπεδο κυβερνοασφάλειας άλλων κρατών μελών, ιδίως λόγω των έντονων 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. Παρόμοια απόκλιση ως προς την εφαρμογή σημειώθηκε σε σχέση με τις διατάξεις της εν λόγω οδηγίας που αφορούν 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,

[12] Άρθρο 11 της οδηγίας (ΕΕ) 2016/1148.
[13] Άρθρο 12 της οδηγίας (ΕΕ) 2016/1148.

επηρεάζοντας ιδίως τη διασυνοριακή παροχή υπηρεσιών και το επίπεδο ανθεκτικότητας της κυβερνοασφάλειας λόγω της εφαρμογής διαφορετικών προτύπων. 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 κυρώσεων που είναι καθοριστικής σημασίας 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) Η παρούσα οδηγία δεν θίγει τη δυνατότητα των κρατών μελών να λαμβάνουν τα αναγκαία μέτρα για την προστασία των ουσιωδών συμφερόντων της ασφάλειας τους, τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και τη διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων, σε συμμόρφωση με το δίκαιο της Ένωσης. Σύμφωνα με το άρθρο 346 της ΣΛΕΕ, κανένα κράτος μέλος δεν υποχρεούται να παρέχει πληροφορίες, η γνωστοποίηση των οποίων θα ήταν αντίθετη προς ουσιώδη συμφέροντα της δημόσιας ασφάλειάς του. Σημαντικά στοιχεία στο πλαίσιο αυτό είναι οι εθνικοί και ενωσιακοί κανόνες για την προστασία διαβαθμισμένων πληροφοριών, οι συμφωνίες εμπιστευτικότητας και οι ανεπίσημες συμφωνίες εμπιστευτικότητας, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light Protocol»[14].

(7) Με την κατάργηση της οδηγίας (ΕΕ) 2016/1148, το πεδίο εφαρμογής ανά τομείς θα πρέπει να επεκταθεί σε μεγαλύτερο μέρος της οικονομίας υπό το πρίσμα των εκτιμήσεων που εκτίθενται στις αιτιολογικές σκέψεις (4) έως (6). Ως εκ τούτου, οι τομείς που καλύπτονται από την οδηγία (ΕΕ) 2016/1148 θα πρέπει να επεκταθούν ώστε να παρέχουν ολοκληρωμένη κάλυψη των τομέων και υπηρεσιών ζωτικής σημασίας για βασικές κοινωνιακές και οικονομικές δραστηριότητες εντός της εσωτερικής αγοράς. Οι κανόνες δεν θα πρέπει να διαφέρουν ανάλογα με το αν οι οντότητες είναι φορείς εκμετάλλευσης βασικών υπηρεσιών ή πάροχοι ψηφιακών υπηρεσιών. Η διαφοροποίηση αυτή έχει αποδειχθεί παρωχημένη, δεδομένου ότι δεν αποτυπώνει την πραγματική σημασία των τομέων ή των υπηρεσιών για τις κοινωνιακές και οικονομικές δραστηριότητες στην εσωτερική αγορά.

(8) 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 («διαδικασία προσδιορισμού»). Προκειμένου να εξαλειφθούν οι μεγάλες αποκλίσεις μεταξύ των κρατών μελών ως προς το θέμα αυτό και να εξασφαλιστεί ασφάλεια δικαίου για όλες τις σχετικές οντότητες όσον αφορά τις απαιτήσεις διαχείρισης κινδύνου 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 του κανόνα του κατωτάτου ορίου μεγέθους, σύμφωνα με τον οποίο όλες οι μεσαίες και μεγάλες επιχειρήσεις, όπως ορίζονται στη σύσταση

[14] Το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light» (TLP) είναι μέσο που επιτρέπει σε όσους και όσες ανταλλάσσουν πληροφορίες να ενημερώνουν το ακροατήριό τους σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση των πληροφοριών αυτών. Χρησιμοποιείται σε όλες σχεδόν τις κοινότητες των ομάδων CSIRT και σε ορισμένα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC).

2003/361/ΕΚ της Επιτροπής[15], οι οποίες δραστηριοποιούνται εντός των τομέων ή παρέχουν το είδος των υπηρεσιών που καλύπτονται από την παρούσα οδηγία, εμπίπτουν στο πεδίο εφαρμογής της. Τα κράτη μέλη δεν θα πρέπει να υποχρεούνται να καταρτίσουν κατάλογο των οντοτήτων οι οποίες πληρούν αυτό το γενικά εφαρμοστέο κριτήριο που αφορά το μέγεθος.

(9) Ωστόσο, θα πρέπει επίσης να καλύπτονται από την παρούσα οδηγία οι μικρές ή πολύ μικρές οντότητες που πληρούν ορισμένα κριτήρια τα οποία υποδηλώνουν ότι αυτές διαδραματίζουν βασικό ρόλο στις οικονομίες ή τις κοινωνίες των κρατών μελών ή σε συγκεκριμένους τομείς ή είδη υπηρεσιών. Τα κράτη μέλη θα πρέπει να φέρουν την ευθύνη να καταρτίσουν κατάλογο των εν λόγω οντοτήτων και να τον υποβάλουν στην Επιτροπή.

(10) Η Επιτροπή, σε διαβούλευση με την ομάδα συνεργασίας, μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με την εφαρμογή των κριτηρίων που ισχύουν για τις πολύ μικρές και τις μικρές επιχειρήσεις.

(11) Ανάλογα με τον τομέα στον οποίο δραστηριοποιούνται ή το είδος της υπηρεσίας που παρέχουν, οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να ταξινομηθούν σε δύο κατηγορίες: βασικές και σημαντικές. Η κατηγοριοποίηση αυτή θα πρέπει να λαμβάνει υπόψη το επίπεδο κρισιμότητας του τομέα ή του είδους της υπηρεσίας, καθώς και το επίπεδο εξάρτησης άλλων τομέων ή ειδών υπηρεσιών. Τόσο οι βασικές όσο και οι σημαντικές οντότητες θα πρέπει να υπόκεινται στις ίδιες απαιτήσεις διαχείρισης κινδύνου και στις ίδιες υποχρεώσεις αναφοράς περιστατικών. Τα καθεστώτα εποπτείας και επιβολής κυρώσεων μεταξύ αυτών των δύο κατηγοριών οντοτήτων θα πρέπει να διαφοροποιούνται ώστε να εξασφαλίζεται δίκαιη ισορροπία μεταξύ των απαιτήσεων και των υποχρεώσεων, αφενός, και του διοικητικού φόρτου που προκύπτει από την εποπτεία της συμμόρφωσης, αφετέρου.

(12) Η τομεακή νομοθεσία και τομεακά μέσα μπορούν να συμβάλουν στη διασφάλιση υψηλών επιπέδων κυβερνοασφάλειας, λαμβάνοντας παράλληλα πλήρως υπόψη τις ιδιαιτερότητες και την πολυπλοκότητα των εν λόγω τομέων. Όταν μια τομεακή νομική πράξη της Ένωσης επιβάλλει σε βασικές ή σημαντικές οντότητες υποχρεώσεις εφαρμογής μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας ή κοινοποίησης περιστατικών ή σημαντικών κυβερνοαπειλών οι οποίες έχουν τουλάχιστον ισοδύναμο αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, θα πρέπει να εφαρμόζονται οι εν λόγω τομεακές διατάξεις, μεταξύ άλλων σχετικά με την εποπτεία και την επιβολή. Η Επιτροπή μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με την εφαρμογή του lex specialis. Η παρούσα οδηγία δεν αποκλείει την έκδοση πρόσθετων τομεακών πράξεων της Ένωσης σχετικά με μέτρα διαχείρισης κινδύνου και κοινοποιήσεις περιστατικών στον τομέα της κυβερνοασφάλειας. Η παρούσα οδηγία δεν θίγει τις υφιστάμενες εκτελεστικές αρμοδιότητες που έχουν ανατεθεί στην Επιτροπή σε διάφορους τομείς, συμπεριλαμβανομένων των μεταφορών και της ενέργειας.

(13) Ο κανονισμός XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[16] 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

---

15 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).

16 *[να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]*

που θεσπίζονται δυνάμει της παρούσας οδηγίας, θα πρέπει να εφαρμόζονται οι διατάξεις του κανονισμού XXXX/XXXX σχετικά με τα μέτρα διαχείρισης κινδύνων της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ), τη διαχείριση περιστατικών που σχετίζονται με τις ΤΠΕ και ιδίως την αναφορά περιστατικών, 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 κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας, την ανταλλαγή πληροφοριών και την εποπτεία, καθώς και την επιβολή της νομοθεσίας στις χρηματοπιστωτικές οντότητες που καλύπτονται από τον κανονισμό XXXX/XXXX. Ταυτόχρονα, είναι σημαντικό να διατηρηθεί στενή σχέση και ανταλλαγή πληροφοριών με τον χρηματοπιστωτικό τομέα στο πλαίσιο της παρούσας οδηγίας. Προς τον σκοπό αυτό, ο κανονισμός XXXX/XXXX επιτρέπει σε όλες τις χρηματοπιστωτικές εποπτικές αρχές, στις Ευρωπαϊκές Εποπτικές Αρχές (ΕΕΑ) για τον χρηματοπιστωτικό τομέα και στις εθνικές αρμόδιες αρχές δυνάμει του κανονισμού XXXX/XXXX να συμμετέχουν στις συζητήσεις στρατηγικής πολιτικής και στις τεχνικές εργασίες της ομάδας συνεργασίας, καθώς και να ανταλλάσσουν πληροφορίες και να συνεργάζονται τόσο με τα ενιαία σημεία επαφής που ορίζονται δυνάμει της παρούσας οδηγίας όσο και με τις εθνικές CSIRT. Οι αρμόδιες αρχές δυνάμει του κανονισμού XXXX/XXXX θα πρέπει να διαβιβάζουν λεπτομερή στοιχεία για σημαντικά περιστατικά που σχετίζονται με τις ΤΠΕ και στα ενιαία σημεία επαφής που ορίζονται δυνάμει της παρούσας οδηγίας. Επιπλέον, τα κράτη μέλη θα πρέπει να συνεχίσουν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις στρατηγικές τους για την κυβερνοασφάλεια, και οι εθνικές CSIRT μπορούν να περιλαμβάνουν τον χρηματοπιστωτικό τομέα στις δραστηριότητές τους.

(14) Λαμβανομένων υπόψη των διασυνδέσεων μεταξύ της κυβερνοασφάλειας και της φυσικής ασφάλειας των οντοτήτων, θα πρέπει να εξασφαλιστεί μια συνεκτική προσέγγιση μεταξύ της οδηγίας (ΕΕ) XXX/XXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17] και της παρούσας οδηγίας. Για να επιτευχθεί αυτό, τα κράτη μέλη θα πρέπει να διασφαλίσουν ότι οι κρίσιμες οντότητες και οι ισοδύναμες οντότητες, σύμφωνα με την οδηγία (ΕΕ) XXX/XXX, θεωρούνται βασικές οντότητες δυνάμει της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει επίσης να διασφαλίζουν ότι οι στρατηγικές τους για την κυβερνοασφάλεια παρέχουν ένα πλαίσιο πολιτικής για ενισχυμένο συντονισμό μεταξύ της αρμόδιας αρχής δυνάμει της παρούσας οδηγίας και της αρμόδιας αρχής δυνάμει της οδηγίας (ΕΕ) XXX/XXX στο πλαίσιο της ανταλλαγής πληροφοριών σχετικά με περιστατικά και κυβερνοαπειλές και της άσκησης εποπτικών καθηκόντων. Οι αρχές δυνάμει και των δύο οδηγιών θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες, ιδίως σε σχέση με τον εντοπισμό κρίσιμων οντοτήτων, τις κυβερνοαπειλές, τους κινδύνους κυβερνοασφάλειας, τα περιστατικά που επηρεάζουν κρίσιμες οντότητες, καθώς και σε σχέση με τα μέτρα κυβερνοασφάλειας που λαμβάνονται από κρίσιμες οντότητες. Κατόπιν αιτήματος των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) XXX/XXX, οι αρμόδιες αρχές δυνάμει της παρούσας οδηγίας θα πρέπει να έχουν τη δυνατότητα να ασκούν τις εποπτικές και εκτελεστικές εξουσίες τους σε βασική οντότητα που προσδιορίζεται ως κρίσιμη. Και οι δύο αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες προς τον σκοπό αυτό.

[17] *[να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]*

(15) Η υποστήριξη και η διατήρηση ενός αξιόπιστου, ανθεκτικού και ασφαλούς συστήματος ονομάτων τομέα (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. Ως εκ τούτου, η παρούσα οδηγία θα πρέπει να εφαρμόζεται σε όλους τους παρόχους υπηρεσιών DNS κατά μήκος της αλυσίδας επίλυσης DNS, συμπεριλαμβανομένων των διαχειριστών των εξυπηρετητών ονομάτων ρίζας (root name servers), των διακομιστών ονομάτων τομέα ανωτάτου επιπέδου (TLD), των επίσημων διακομιστών ονομάτων για ονόματα τομέα και των αναδρομικών επιλυτών.

(16) Οι υπηρεσίες νεφοϋπολογιστικής θα πρέπει να καλύπτουν τις υπηρεσίες που επιτρέπουν κατά παραγγελία και ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενο και ελαστικό σύνολο κοινόχρηστων και κατανεμημένων υπολογιστικών πόρων. Οι εν λόγω υπολογιστικοί πόροι περιλαμβάνουν πόρους όπως δίκτυα, εξυπηρετητές ή άλλες υποδομές, λειτουργικά συστήματα, λογισμικό, αποθήκευση, εφαρμογές και υπηρεσίες. Τα μοντέλα ανάπτυξης της νεφοϋπολογιστικής θα πρέπει να περιλαμβάνουν το ιδιωτικό, το κοινοτικό, το δημόσιο και το υβριδικό υπολογιστικό νέφος. Τα προαναφερθέντα μοντέλα υπηρεσιών και ανάπτυξης έχουν την ίδια έννοια με τους όρους παροχής υπηρεσίας και μοντέλα ανάπτυξης που ορίζονται στο πρότυπο ISO/IEC 17788:2014. Η ικανότητα του χρήστη του υπολογιστικού νέφους να παρέχει 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 την κατάσταση κατά την οποία οι ικανότητες υπολογιστικού νέφους παρέχονται μέσω του δικτύου και η πρόσβαση σε αυτές γίνεται μέσω μηχανισμών που προωθούν τη χρήση ετερογενών πλατφορμών, λεπτών ή παχιών πελατών (συμπεριλαμβανομένων κινητών τηλεφώνων, ταμπλετών, φορητών υπολογιστών, 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 εκείνους τους υπολογιστικούς πόρους που διατίθενται και απελευθερώνονται ανάλογα με τη ζήτηση προκειμένου να καταστεί δυνατή η ταχεία αύξηση και μείωση των διαθέσιμων πόρων ανάλογα με τον φόρτο εργασίας. Ο όρος «κοινόχρηστοι» χρησιμοποιείται για να περιγράψει εκείνους τους υπολογιστικούς πόρους που παρέχονται σε πολλούς χρήστες που διαθέτουν από κοινού την πρόσβαση στην υπηρεσία, αλλά η επεξεργασία εκτελείται χωριστά για κάθε χρήστη, παρόλο που η υπηρεσία παρέχεται από τον ίδιο ηλεκτρονικό εξοπλισμό. Ο όρος «κατανεμημένοι» χρησιμοποιείται για να περιγράψει τους υπολογιστικούς πόρους που βρίσκονται σε διαφορετικούς δικτυωμένους υπολογιστές ή συσκευές και οι οποίοι επικοινωνούν και συντονίζονται μεταξύ τους μέσω διαβίβασης μηνυμάτων.

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

(18) Οι υπηρεσίες που παρέχονται από τους παρόχους υπηρεσιών κέντρων δεδομένων ενδέχεται να μην παρέχονται πάντοτε με τη μορφή υπηρεσιών νεφοϋπολογιστικής. Ως εκ τούτου, τα κέντρα δεδομένων ενδέχεται να μην αποτελούν πάντοτε μέρος της υποδομής νεφοϋπολογιστικής. Για τη διαχείριση όλων των κινδύνων για την ασφάλεια δικτυακών και πληροφοριακών συστημάτων, η παρούσα οδηγία θα πρέπει να καλύπτει επίσης τους παρόχους τέτοιων υπηρεσιών κέντρων δεδομένων που δεν είναι υπηρεσίες νεφοϋπολογιστικής. 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 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 ισχύει για ενδοεπιχειρησιακά, εταιρικά κέντρα δεδομένων που ανήκουν και λειτουργούν για ίδιους σκοπούς της οικείας οντότητας.

(19) Οι φορείς παροχής ταχυδρομικών υπηρεσιών κατά την έννοια της οδηγίας 97/67/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[18], καθώς και οι πάροχοι υπηρεσιών επείγουσας παράδοσης και ταχυμεταφορών, 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 ή τη διανομή, συμπεριλαμβανομένων των υπηρεσιών παραλαβής. Οι υπηρεσίες μεταφορών που δεν αναλαμβάνονται σε συνδυασμό με ένα από τα στάδια αυτά θα πρέπει να μείνουν εκτός του πεδίου των ταχυδρομικών υπηρεσιών.

(20) Αυτές οι αυξανόμενες αλληλεξαρτήσεις είναι αποτέλεσμα ενός ολοένα και περισσότερο διασυνοριακού και αλληλεξαρτώμενου δικτύου παροχής υπηρεσιών που χρησιμοποιεί βασικές υποδομές σε ολόκληρη την Ένωση στους τομείς 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 διαταραχή, 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. Η πανδημία της COVID-19 κατέδειξε την τρωτότητα των ολοένα και πιο αλληλεξαρτώμενων κοινωνιών μας απέναντι σε κινδύνους χαμηλής πιθανότητας.

(21) Με δεδομένες τις διαφορές των εθνικών δομών 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 ορίζουν περισσότερες από μία αρμόδιες εθνικές αρχές για την εκτέλεση των καθηκόντων που συνδέονται με την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων

[18] 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).

βασικών και σημαντικών οντοτήτων δυνάμει της παρούσας οδηγίας. Τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να αναθέτουν τον ρόλο αυτόν σε υφιστάμενη αρχή.

(22) 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 εθνικό ενιαίο σημείο επαφής υπεύθυνο για τον συντονισμό θεμάτων σχετικά με την ασφάλεια δικτυακών και πληροφοριακών συστημάτων και με τη διασυνοριακή συνεργασία σε επίπεδο Ένωσης.

(23) Οι αρμόδιες αρχές ή οι ομάδες CSIRT θα πρέπει να λαμβάνουν με αποτελεσματικό και αποδοτικό τρόπο τις κοινοποιήσεις περιστατικών από τις οντότητες. Τα ενιαία σημεία επαφής θα πρέπει να είναι επιφορτισμένα με τη διαβίβαση των κοινοποιήσεων περιστατικών στα ενιαία κέντρα επαφής άλλων επηρεαζόμενων κρατών μελών. Στο επίπεδο των αρχών των κρατών μελών, για να εξασφαλιστεί ένα ενιαίο σημείο εισόδου σε κάθε κράτος μέλος, τα ενιαία σημεία επαφής θα πρέπει να είναι επίσης οι αποδέκτες των σχετικών πληροφοριών σχετικά με περιστατικά που αφορούν οντότητες του χρηματοπιστωτικού τομέα από τις αρμόδιες αρχές δυνάμει του κανονισμού XXXX/XXXX, τις οποίες θα πρέπει να μπορούν να διαβιβάζουν, κατά περίπτωση, στις σχετικές εθνικές αρμόδιες αρχές ή στις CSIRT δυνάμει της παρούσας οδηγίας.

(24) Τα κράτη μέλη θα πρέπει να διαθέτουν τον κατάλληλο εξοπλισμό, τόσο σε τεχνικές όσο και σε οργανωτικές ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση και τον μετριασμό περιστατικών και κινδύνων σε δικτυακά και πληροφοριακά συστήματα. Τα κράτη μέλη θα πρέπει επομένως να φροντίσουν να διαθέτουν εύρυθμα λειτουργούσες CSIRT, γνωστές επίσης ως «ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams – CERT), οι οποίες να συμμορφώνονται με τις βασικές απαιτήσεις ώστε να διασφαλίζεται τόσο η ύπαρξη αποτελεσματικών και συμβατών ικανοτήτων αντιμετώπισης περιστατικών και κινδύνων όσο και η αποτελεσματική συνεργασία σε ενωσιακό επίπεδο. 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 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.

(25) Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, οι CSIRT θα πρέπει να είναι σε θέση να παρέχουν, σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[19] όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, εξ ονόματος και κατόπιν αιτήματος οντότητας δυνάμει της παρούσας οδηγίας, προδραστική σάρωση των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούνται για την παροχή των υπηρεσιών τους. Τα κράτη μέλη θα πρέπει να στοχεύουν στην εξασφάλιση του ίδιου επιπέδου τεχνικών ικανοτήτων για όλες τις τομεακές CSIRT. Για την ανάπτυξη των εθνικών τους CSIRT, τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA).

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

(26) 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.

(27) Σύμφωνα με το παράρτημα της σύστασης (ΕΕ) 2017/1548 της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο («προσχέδιο»)[20], ως περιστατικό μεγάλης κλίμακας θα πρέπει να νοείται εκείνο που έχει ευρείες συνέπειες σε τουλάχιστον δύο κράτη μέλη ή το οποίο προκαλεί διαταραχή που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή. Ανάλογα με την αιτία και τις συνέπειές τους, τα περιστατικά μεγάλης κλίμακας ενδέχεται να κλιμακωθούν και να μετατραπούν σε πραγματικές κρίσεις που καθιστούν αδύνατη την ομαλή λειτουργία της εσωτερικής αγοράς. Δεδομένου των ευρέων 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.

(28) Δεδομένου ότι η εκμετάλλευση των τρωτών σημείων στα δικτυακά και πληροφοριακά συστήματα μπορεί να προκαλέσει σημαντικές διαταραχές και βλάβες, ο άμεσος εντοπισμός και η διόρθωση αυτών των τρωτών σημείων αποτελεί σημαντικό παράγοντα για τη μείωση του κινδύνου για την κυβερνοασφάλεια. Οι οντότητες που αναπτύσσουν τέτοια συστήματα θα πρέπει, ως εκ τούτου, να θεσπίσουν κατάλληλες διαδικασίες για την αντιμετώπιση των τρωτών σημείων όταν εντοπίζονται. Δεδομένου ότι τα τρωτά σημεία συχνά εντοπίζονται και αναφέρονται (γνωστοποιούνται) από τρίτους (αναφέρουσες οντότητες), 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 τρωτά σημεία. Στο πλαίσιο αυτό, τα διεθνή πρότυπα ISO/IEC 30111 και ISO/IEC 29417 παρέχουν καθοδήγηση σχετικά με τον χειρισμό τρωτών σημείων και τη γνωστοποίηση τρωτών σημείων, αντίστοιχα. Όσον αφορά τη γνωστοποίηση τρωτών σημείων, είναι ιδιαίτερα σημαντικός ο συντονισμός μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων ή υπηρεσιών ΤΠΕ. Η συντονισμένη γνωστοποίηση τρωτών σημείων προσδιορίζει μια διαρθρωμένη διαδικασία μέσω της οποίας τα τρωτά σημεία αναφέρονται σε οργανισμούς κατά τρόπο που να επιτρέπει στον οργανισμό να διαγνώσει και να διορθώσει το τρωτό σημείο πριν να αποκαλυφθούν σε τρίτα μέρη ή στο ευρύ κοινό λεπτομερείς πληροφορίες σχετικά με τα τρωτά σημεία. Η συντονισμένη γνωστοποίηση τρωτών σημείων θα πρέπει επίσης να περιλαμβάνει τον συντονισμό μεταξύ της αναφέρουσας οντότητας και του οργανισμού όσον αφορά το χρονοδιάγραμμα διόρθωσης και δημοσιοποίησης των τρωτών σημείων.

(29) Ως εκ τούτου, τα κράτη μέλη οφείλουν να λάβουν μέτρα για να διευκολύνουν τη συντονισμένη γνωστοποίηση τρωτών σημείων με τη θέσπιση σχετικής εθνικής πολιτικής. Στο πλαίσιο αυτό, τα κράτη μέλη θα πρέπει να ορίσουν μια CSIRT η οποία θα αναλάβει ρόλο «συντονίστριας», ενεργώντας ως διαμεσολαβήτρια μεταξύ των αναφερουσών οντοτήτων και των κατασκευαστών ή παρόχων προϊόντων ή υπηρεσιών ΤΠΕ, όπου απαιτείται. Τα καθήκοντα της συντονίστριας CSIRT θα πρέπει να περιλαμβάνουν ιδίως τον προσδιορισμό και την επικοινωνία με τις σχετικές

[20] 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).

οντότητες, την υποστήριξη των αναφερουσών οντοτήτων, τη διαπραγμάτευση των χρονοδιαγραμμάτων γνωστοποίησης και τη διαχείριση των τρωτών σημείων που επηρεάζουν πολλαπλούς οργανισμούς (γνωστοποίηση τρωτών σημείων που αφορούν πολλά μέρη). Όταν τα τρωτά σημεία επηρεάζουν αρκετούς κατασκευαστές ή παρόχους προϊόντων ή υπηρεσιών ΤΠΕ που είναι εγκατεστημένοι σε περισσότερα του ενός κράτη μέλη, οι CSIRT που έχει ορίσει καθένα από τα επηρεαζόμενα κράτη μέλη θα πρέπει να συνεργάζονται στο πλαίσιο του δικτύου CSIRT.

(30) Η πρόσβαση σε ορθές και έγκαιρες πληροφορίες σχετικά με τα τρωτά σημεία που επηρεάζουν τα προϊόντα και τις υπηρεσίες ΤΠΕ συμβάλλει στην ενίσχυση της διαχείρισης κινδύνων κυβερνοασφάλειας. Στο πλαίσιο αυτό, οι πηγές δημόσια διαθέσιμων πληροφοριών σχετικά με τα τρωτά σημεία αποτελούν σημαντικό εργαλείο για τις οντότητες και τους χρήστες τους, αλλά και για τις εθνικές αρμόδιες αρχές και τις CSIRT. Για τον λόγο αυτό, ο ENISA θα πρέπει να καταρτίσει μητρώο τρωτών σημείων στο οποίο βασικές και σημαντικές οντότητες και οι πάροχοί τους, καθώς και οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας, θα μπορούν, σε εθελοντική βάση, να γνωστοποιούν τρωτά σημεία και να παρέχουν τις πληροφορίες σχετικά με τρωτά σημεία οι οποίες επιτρέπουν στους χρήστες να λάβουν κατάλληλα μέτρα μετριασμού.

(31) Μολονότι υπάρχουν παρόμοια μητρώα ή βάσεις δεδομένων τρωτών σημείων, αυτά φιλοξενούνται και τηρούνται από οντότητες που δεν είναι εγκατεστημένες στην Ένωση. Ένα ευρωπαϊκό μητρώο τρωτών σημείων που θα τηρείται από τον ENISA θα προσέφερε βελτιωμένη διαφάνεια όσον αφορά τη διαδικασία δημοσίευσης πριν από την επίσημη γνωστοποίηση του τρωτού σημείου, καθώς και ανθεκτικότητα σε περιπτώσεις διαταραχών ή διακοπών της παροχής παρόμοιων υπηρεσιών. Για να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να επιδιωχθεί η συμπληρωματικότητα στο μέτρο του δυνατού, ο ENISA θα πρέπει να εξετάσει τη δυνατότητα σύναψης συμφωνιών διαρθρωμένης συνεργασίας με παρόμοια μητρώα σε δικαιοδοσίες τρίτων χωρών.

(32) Η ομάδα συνεργασίας θα πρέπει να καταρτίζει ανά διετία πρόγραμμα εργασίας, συμπεριλαμβανομένων των δράσεων που πρέπει να αναληφθούν από την ομάδα για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα του πρώτου προγράμματος που θα εγκριθεί δυνάμει της παρούσας οδηγίας θα πρέπει να ευθυγραμμίζεται με το χρονοδιάγραμμα του τελευταίου προγράμματος που εγκρίθηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148, ώστε να αποφευχθούν ενδεχόμενες διαταραχές στις εργασίες της ομάδας.

(33) Κάθε φορά που καταρτίζει έγγραφα καθοδήγησης, η ομάδα συνεργασίας θα πρέπει: να καταγράφει τις εθνικές λύσεις και εμπειρίες, να αξιολογεί τον αντίκτυπο των παραδοτέων της ομάδας συνεργασίας στις εθνικές προσεγγίσεις, να συζητά τις προκλήσεις όσον αφορά την εφαρμογή και να διατυπώνει ειδικές συστάσεις που πρέπει να λαμβάνονται υπόψη μέσω της καλύτερης εφαρμογής των υφιστάμενων κανόνων.

(34) 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 πρέπει να διοργανώνει τακτικές κοινές συνεδριάσεις με σχετικούς ιδιωτικούς ενδιαφερόμενους φορείς από ολόκληρη την Ένωση για να συζητά δραστηριότητες που πραγματοποιεί η ομάδα και να συγκεντρώνει στοιχεία σχετικά με αναδυόμενες προκλήσεις πολιτικής. Προκειμένου να ενισχύσει τη συνεργασία σε επίπεδο Ένωσης,

η ομάδα θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλέσει για να συμμετάσχουν στις εργασίες της φορείς και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα (EC3), ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας (EASA) και ο Οργανισμός της Ευρωπαϊκής Ένωσης για το Διαστημικό Πρόγραμμα (EUSPA).

(35) Οι αρμόδιες αρχές και οι CSIRT θα πρέπει να εξουσιοδοτηθούν να συμμετέχουν σε προγράμματα ανταλλαγής υπαλλήλων από άλλα κράτη μέλη με σκοπό τη βελτίωση της συνεργασίας. 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.

(36) Η Ένωση θα πρέπει, κατά περίπτωση, να συνάπτει διεθνείς συμφωνίες σύμφωνα με το άρθρο 218 ΣΛΕΕ με τρίτες χώρες ή διεθνείς οργανισμούς επιτρέποντας και οργανώνοντας τη συμμετοχή τους σε ορισμένες δραστηριότητες της ομάδας συνεργασίας και του δικτύου CSIRT. Οι συμφωνίες αυτές θα πρέπει να διασφαλίζουν την επαρκή προστασία των δεδομένων.

(37) 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 μέσω των υφιστάμενων δικτύων συνεργασίας, ιδίως μέσω του δικτύου οργανώσεων διασύνδεσης για τις 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. Οι διαδικαστικοί κανόνες του EU-CyCLONe θα πρέπει να προσδιορίζουν περαιτέρω τις λεπτομέρειες λειτουργίας του δικτύου, συμπεριλαμβανομένων, μεταξύ άλλων, των ρόλων, των τρόπων συνεργασίας, των αλληλεπιδράσεων 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 για την πολιτική αντιμετώπιση κρίσεων (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 (ΚΠΑΑ), θα πρέπει να ενεργοποιείται ο Μηχανισμός Αντιμετώπισης Κρίσεων (CRM) της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ).

(38) Για τους σκοπούς της παρούσας οδηγίας, ο όρος «κίνδυνος» θα πρέπει να αναφέρεται στην πιθανότητα απώλειας ή διαταραχής που προκαλείται από περιστατικό κυβερνοασφάλειας και θα πρέπει να εκφράζεται ως συνδυασμός του μεγέθους της εν λόγω απώλειας ή διαταραχής και της πιθανότητας επέλευσης του εν λόγω περιστατικού.

(39) Για τους σκοπούς της παρούσας οδηγίας, ο όρος «παρ' ολίγον περιστατικά» θα πρέπει να αναφέρεται σε ένα γεγονός το οποίο θα μπορούσε δυνητικά να προκαλέσει βλάβη, αλλά του οποίου η συντέλεση εμποδίστηκε επιτυχώς.

(40) Τα μέτρα για τη διαχείριση του κινδύνου θα πρέπει να περιλαμβάνουν μέτρα για τον εντοπισμό των τυχόν κινδύνων περιστατικών, καθώς και μέτρα για την πρόληψη, την ανίχνευση και την αντιμετώπιση περιστατικών και για τον μετριασμό του αντίκτυπού τους. Η ασφάλεια δικτυακών και πληροφοριακών συστημάτων θα πρέπει να περιλαμβάνει την ασφάλεια των δεδομένων που αποθηκεύονται, μεταδίδονται και υποβάλλονται σε επεξεργασία.

(41) Για να αποφευχθεί η δυσανάλογη οικονομική και διοικητική επιβάρυνση των βασικών και των σημαντικών οντοτήτων, οι απαιτήσεις σχετικά με τη διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει να είναι ανάλογες προς τον κίνδυνο που ενέχει το σχετικό δικτυακό και πληροφοριακό σύστημα, λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων όσον αφορά τα σχετικά μέτρα.

(42) Οι βασικές και οι σημαντικές οντότητες θα πρέπει να εγγυώνται την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν στις δραστηριότητές τους. Κατά κύριο λόγο πρόκειται για ιδιωτικά δικτυακά και πληροφοριακά συστήματα τα οποία διαχειρίζεται το εσωτερικά απασχολούμενο προσωπικό πληροφορικής ή των οποίων η ασφάλεια έχει ανατεθεί σε τρίτους. Οι απαιτήσεις για τη διαχείριση των κινδύνων και την αναφορά περιστατικών σχετικά με την κυβερνοασφάλεια σύμφωνα με την παρούσα οδηγία θα πρέπει να εφαρμόζονται στις σχετικές βασικές και σημαντικές οντότητες, ανεξάρτητα από το αν εκτελούν τη συντήρηση των δικτυακών και πληροφοριακών συστημάτων τους εσωτερικά ή αν την αναθέτουν σε τρίτους.

(43) Η αντιμετώπιση των κινδύνων κυβερνοασφάλειας που γεννώνται από την αλυσίδα εφοδιασμού μιας οντότητας και τη σχέση της με τους προμηθευτές της είναι ιδιαίτερα σημαντική, δεδομένης της συχνής εμφάνισης περιστατικών κατά τα οποία οι οντότητες καθίστανται θύματα κυβερνοεπιθέσεων και στα οποία κακόβουλοι παράγοντες κατόρθωσαν να θέσουν σε κίνδυνο την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων μιας οντότητας εκμεταλλευόμενοι τρωτά σημεία που επηρεάζουν προϊόντα και υπηρεσίες τρίτων. Ως εκ τούτου, οι οντότητες θα πρέπει να αξιολογούν και να λαμβάνουν υπόψη τη συνολική ποιότητα των προϊόντων και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών τους διαδικασιών ανάπτυξης.

(44) Μεταξύ των παρόχων υπηρεσιών, οι πάροχοι υπηρεσιών διαχείρισης της ασφάλειας (managed security services providers – MSSP) 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 τον εντοπισμό και την αντιμετώπιση περιστατικών. Ωστόσο, οι ίδιοι οι MSSP αυτοί αποτελούν επίσης στόχους κυβερνοεπιθέσεων και, μέσω της στενής ενσωμάτωσής τους στις λειτουργίες των φορέων εκμετάλλευσης, συνιστούν ιδιαίτερο κίνδυνο για την κυβερνοασφάλεια. Ως εκ τούτου, οι οντότητες θα πρέπει να επιδεικνύουν αυξημένη επιμέλεια κατά την επιλογή ενός MSSP.

(45) Οι οντότητες θα πρέπει επίσης να αντιμετωπίζουν τους κινδύνους για την κυβερνοασφάλεια που γεννώνται από τις αλληλεπιδράσεις και τις σχέσεις τους με άλλα ενδιαφερόμενα μέρη εντός ενός ευρύτερου οικοσυστήματος. Ειδικότερα, οι 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 διανοητικής ιδιοκτησίας ειδικότερα. Ομοίως, δεδομένης της σημασίας και της αξίας που έχουν τα δεδομένα για τις δραστηριότητες των οντοτήτων, όταν βασίζονται σε υπηρεσίες μετασχηματισμού και ανάλυσης δεδομένων από τρίτα μέρη, οι οντότητες θα πρέπει να λαμβάνουν όλα τα κατάλληλα μέτρα κυβερνοασφάλειας.

(46) Για την περαιτέρω αντιμετώπιση των βασικών κινδύνων της αλυσίδας εφοδιασμού και την παροχή βοήθειας σε οντότητες οι οποίες δραστηριοποιούνται σε τομείς που καλύπτονται από την παρούσα οδηγία με σκοπό την κατάλληλη διαχείριση των κινδύνων για την κυβερνοασφάλεια που σχετίζονται με την αλυσίδα εφοδιασμού και

τους προμηθευτές, η ομάδα συνεργασίας στην οποία συμμετέχουν αρμόδιες εθνικές αρχές, σε συνεργασία με την Επιτροπή και τον ENISA, θα πρέπει να διενεργεί συντονισμένες τομεακές εκτιμήσεις κινδύνου στην αλυσίδα εφοδιασμού, όπως έγινε ήδη για τα δίκτυα 5G κατόπιν της σύστασης (ΕΕ) 2019/534 για την κυβερνοασφάλεια των δικτύων 5G[21], με στόχο τον εντοπισμό ανά τομέα των κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ, των σχετικών απειλών και των τρωτών σημείων.

(47) Οι εκτιμήσεις κινδύνου στην αλυσίδα εφοδιασμού, υπό το πρίσμα 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, 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, συστήματα ή προϊόντα ΤΠΕ· ii) τη σημασία συγκεκριμένων κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ για την εκτέλεση κρίσιμων ή ευαίσθητων λειτουργιών, συμπεριλαμβανομένης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· iii) τη διαθεσιμότητα εναλλακτικών υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ· iv) την ανθεκτικότητα του συνόλου της αλυσίδας εφοδιασμού υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ έναντι γεγονότων που προκαλούν διαταραχές και v) όσον αφορά αναδυόμενες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ, τη δυνητική μελλοντική τους σημασία για τις δραστηριότητες των οντοτήτων.

(48) Για τον εξορθολογισμό των νομικών υποχρεώσεων που επιβάλλονται στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και στους παρόχους υπηρεσιών εμπιστοσύνης που σχετίζονται με την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων, καθώς και για να δοθεί η δυνατότητα στις εν λόγω οντότητες και στις αντίστοιχες αρμόδιες αρχές τους να επωφεληθούν από το νομικό πλαίσιο που θεσπίζεται με την παρούσα οδηγία (συμπεριλαμβανομένου του ορισμού των CSIRT που είναι υπεύθυνες για τον χειρισμό κινδύνων και περιστατικών, της συμμετοχής των αρμόδιων αρχών και φορέων στις εργασίες της ομάδας συνεργασίας και του δικτύου CSIRT), θα πρέπει να συμπεριληφθούν στο πεδίο εφαρμογής της παρούσας οδηγίας. Συνεπώς, οι αντίστοιχες διατάξεις του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[22] και της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[23] σχετικά με την επιβολή απαιτήσεων ασφάλειας και κοινοποίησης σε αυτούς τους τύπους οντοτήτων, θα πρέπει να καταργηθούν. Οι κανόνες σχετικά με τις υποχρεώσεις αναφοράς περιστατικών δεν θα πρέπει να θίγουν

---

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

22 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).

23 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).

τον κανονισμό (ΕΕ) 2016/679 και την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24].

(49) Κατά περίπτωση, και για την αποφυγή περιττών διαταραχών, οι υφιστάμενες εθνικές κατευθυντήριες γραμμές και η εθνική νομοθεσία που έχουν θεσπιστεί για τη μεταφορά στο εθνικό δίκαιο των κανόνων σχετικά με τα μέτρα ασφάλειας που ορίζονται στο άρθρο 40 παράγραφος 1 της οδηγίας (ΕΕ) 2018/1972, καθώς και των απαιτήσεων του άρθρου 40 παράγραφος 2 της εν λόγω οδηγίας σχετικά με τις παραμέτρους που σχετίζονται με τη σημασία ενός περιστατικού, θα πρέπει να συνεχίσουν να χρησιμοποιούνται από τις αρμόδιες αρχές που είναι επιφορτισμένες με την εποπτεία και την επιβολή για τους σκοπούς της παρούσας οδηγίας.

(50) Δεδομένης της αυξανόμενης σημασίας των υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών, 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. Οι πάροχοι των εν λόγω υπηρεσιών θα πρέπει, συνεπώς, να διασφαλίζουν επίσης ένα επίπεδο ασφάλειας των δικτυακών και πληροφοριακών συστημάτων, ανάλογο προς τον εκάστοτε κίνδυνο. Δεδομένου ότι οι πάροχοι υπηρεσιών διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών 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 που χρησιμοποιούν αριθμούς και δεν ασκούν πραγματικό έλεγχο επί της μετάδοσης σημάτων.

(51) 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 τα δημόσια δίκτυα ηλεκτρονικών επικοινωνιών, όπως, για παράδειγμα, οι βασικοί κορμοί του διαδικτύου ή τα υποβρύχια καλώδια επικοινωνιών, να διαθέτουν κατάλληλα μέτρα κυβερνοασφάλειας και να αναφέρουν τα σχετικά περιστατικά.

(52) Κατά περίπτωση, οι οντότητες θα πρέπει να ενημερώνουν τους αποδέκτες των υπηρεσιών τους για συγκεκριμένες και σημαντικές απειλές και για τα μέτρα που μπορούν να λάβουν για να μετριάσουν τον, τυχόν, συνεπαγόμενο για αυτές κίνδυνο. Η απαίτηση να ενημερώνονται οι εν λόγω αποδέκτες σχετικά με τέτοιες απειλές, δεν θα πρέπει να απαλλάσσει τις οντότητες από την υποχρέωση να λαμβάνουν, με ίδιες δαπάνες, κατάλληλα και άμεσα μέτρα για την αποτροπή κυβερνοαπειλών ή την επανόρθωση τυχόν συνεπειών τους και για την αποκατάσταση του κανονικού επιπέδου ασφάλειας. Η σχετική ενημέρωση προς τους αποδέκτες σχετικά με απειλές για την ασφάλεια θα πρέπει να παρέχεται δωρεάν.

(53) Ειδικότερα, οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών θα πρέπει να ενημερώνουν τους αποδέκτες υπηρεσιών σχετικά με ιδιαίτερες και σημαντικές κυβερνοαπειλές και

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

σχετικά με τα μέτρα προστασίας που μπορούν να λαμβάνουν για την ασφάλεια των επικοινωνιών τους, για παράδειγμα χρησιμοποιώντας συγκεκριμένους τύπους λογισμικού ή τεχνολογίες κρυπτογράφησης.

(54) Προκειμένου να διαφυλαχθεί η ασφάλεια των δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών , θα πρέπει να προωθηθεί η χρήση της κρυπτογράφησης, και ιδίως της διατερματικής κρυπτογράφησης, και, όπου απαιτείται, αυτή θα πρέπει να είναι υποχρεωτική για τους παρόχους των εν λόγω υπηρεσιών και δικτύων, σύμφωνα με τις αρχές της ασφάλειας και της ιδιωτικότητας εκ προεπιλογής και εκ σχεδιασμού, για τους σκοπούς του άρθρου 18. 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 τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων σύμφωνα με το δίκαιο της Ένωσης. Οι λύσεις για τη νόμιμη πρόσβαση σε πληροφορίες σε διατερματικές κρυπτογραφημένες επικοινωνίες θα πρέπει να διατηρούν την αποτελεσματικότητα της κρυπτογράφησης όσον αφορά την προστασία της ιδιωτικής ζωής και της ασφάλειας των επικοινωνιών, παρέχοντας παράλληλα αποτελεσματική άμυνα κατά της εγκληματικότητας.

(55) Η παρούσα οδηγία θεσπίζει μια προσέγγιση δύο σταδίων ως προς την αναφορά περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς, που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης συμβάντων και επιτρέπει στις 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 ανθεκτικότητα μεμονωμένων εταιρειών και ολόκληρων τομέων έναντι των κυβερνοαπειλών. Όταν οι οντότητες λαμβάνουν γνώση περιστατικού, θα πρέπει να υποχρεούνται να υποβάλουν αρχική κοινοποίηση εντός 24 ωρών, ακολουθούμενη από τελική έκθεση το αργότερο ένα μήνα μετά. Η αρχική κοινοποίηση θα πρέπει να περιλαμβάνει μόνο τις πληροφορίες που είναι απολύτως αναγκαίες για να ενημερωθούν οι αρμόδιες αρχές σχετικά με το περιστατικό και να δοθεί η δυνατότητα στην οντότητα να ζητήσει συνδρομή, εφόσον απαιτείται. Η εν λόγω κοινοποίηση, κατά περίπτωση, θα πρέπει να αναφέρει εάν το περιστατικό είναι πιθανόν να οφείλεται σε παράνομη ή κακόβουλη ενέργεια. Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι η απαίτηση υποβολής αυτής της αρχικής κοινοποίησης δεν εκτρέπει τους πόρους της αναφέρουσας οντότητας από δραστηριότητες που σχετίζονται με τον χειρισμό περιστατικών, στις οποίες θα πρέπει να δίνεται προτεραιότητα. Για να αποτραπεί το μελλοντικό ενδεχόμενο οι υποχρεώσεις αναφοράς περιστατικών είτε να εκτρέπουν πόρους από τον χειρισμό της αντιμετώπισης περιστατικών είτε να μπορούν με άλλον τρόπο να θέσουν σε κίνδυνο τις σχετικές προσπάθειες των φορέων, τα κράτη μέλη θα πρέπει επίσης να προβλέπουν ότι, σε δεόντως αιτιολογημένες περιπτώσεις και σε συμφωνία με τις αρμόδιες αρχές ή την CSIRT, η εν λόγω οντότητα θα μπορεί να παρεκκλίνει από τις προθεσμίες των 24 ωρών για την αρχική κοινοποίηση και του ενός μήνα για την τελική έκθεση.

(56) Οι βασικές και σημαντικές 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 πρόσθετες επιβαρύνσεις και ενδέχεται επίσης να οδηγήσουν σε αβεβαιότητες όσον αφορά τη μορφή και τις διαδικασίες των εν λόγω κοινοποιήσεων. Με βάση τα ανωτέρω και για τους σκοπούς της αναφοράς περιστατικών που θέτουν

σε κίνδυνο την ασφάλεια, τα κράτη μέλη θα πρέπει να θεσπίσουν *ενιαίο σημείο εισόδου* για όλες τις κοινοποιήσεις που απαιτούνται βάσει της παρούσας οδηγίας, καθώς και βάσει άλλων νομοθετικών πράξεων της Ένωσης, όπως ο κανονισμός (ΕΕ) 2016/679 και η οδηγία 2002/58/ΕΚ. Ο ENISA, σε συνεργασία με την ομάδα συνεργασίας, θα πρέπει να αναπτύξει κοινά υποδείγματα κοινοποίησης μέσω κατευθυντήριων γραμμών που θα απλουστεύουν και θα εξορθολογίζουν τις πληροφορίες αναφοράς που απαιτούνται από το δίκαιο της Ένωσης και θα μειώνουν τον φόρτο για τις εταιρείες.

(57) 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 EC3 και από τον ENISA.

(58) Ως αποτέλεσμα περιστατικών, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για όλα τα σχετικά θέματα με τις αρχές προστασίας δεδομένων και τις εποπτικές αρχές, σύμφωνα με την οδηγία 2002/58/ΕΚ.

(59) Η διατήρηση επακριβών και πλήρων βάσεων δεδομένων ονομάτων τομέα και δεδομένων καταχώρισης (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. Όταν η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, η εν λόγω επεξεργασία συμμορφώνεται με το δίκαιο της Ένωσης για την προστασία των δεδομένων.

(60) Η διαθεσιμότητα των εν λόγω δεδομένων για τις δημόσιες αρχές και η έγκαιρη προσβασιμότητά τους από αυτές, συμπεριλαμβανομένων των αρμόδιων αρχών βάσει του ενωσιακού ή του εθνικού δικαίου για την πρόληψη, τη διερεύνηση ή τη δίωξη ποινικών αδικημάτων, των CERT, των CSIRT, και όσον αφορά τα δεδομένα των πελατών τους, σε παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και σε παρόχους τεχνολογιών και υπηρεσιών κυβερνοασφάλειας που ενεργούν για λογαριασμό των εν λόγω πελατών, είναι ουσιαστικής σημασίας για την πρόληψη και την καταπολέμηση της κατάχρησης του συστήματος ονομάτων τομέα, ιδίως για την πρόληψη, τον εντοπισμό και την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Η εν λόγω πρόσβαση θα πρέπει να συμμορφώνεται με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων στον βαθμό που σχετίζεται με δεδομένα προσωπικού χαρακτήρα.

(61) Προκειμένου να διασφαλιστεί η διαθεσιμότητα ακριβών και πλήρων δεδομένων καταχώρισης ονομάτων τομέα, τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD (οι αποκαλούμενοι καταχωρητές), θα πρέπει να συλλέγουν και να εγγυώνται την ακεραιότητα και τη διαθεσιμότητα των δεδομένων καταχώρισης ονομάτων τομέα. Ειδικότερα, τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον

TLD θα πρέπει να θεσπίσουν πολιτικές και διαδικασίες για τη συλλογή και τη διατήρηση ακριβών και πλήρων δεδομένων καταχώρισης, καθώς και για την πρόληψη και διόρθωση ανακριβών δεδομένων καταχώρισης σύμφωνα με τους κανόνες της Ένωσης για την προστασία των δεδομένων.

(62) Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για αυτά θα πρέπει να δημοσιοποιούν δεδομένα καταχώρισης ονομάτων τομέα που δεν εμπίπτουν στο πεδίο εφαρμογής των κανόνων της Ένωσης για την προστασία των δεδομένων, όπως δεδομένα που αφορούν νομικά πρόσωπα[25]. Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD θα πρέπει επίσης να καθιστούν δυνατή τη νόμιμη πρόσβαση από νόμιμους 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 διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για λογαριασμό τους θα πρέπει να ανταποκρίνονται χωρίς αδικαιολόγητη καθυστέρηση σε αιτήματα νόμιμων αιτούντων πρόσβαση για τη γνωστοποίηση δεδομένων καταχώρισης ονομάτων τομέα. Τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για λογαριασμό τους 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 νόμιμους αιτούντες πρόσβαση. Η διαδικασία πρόσβασης μπορεί επίσης 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. Με σκοπό την προώθηση εναρμονισμένων πρακτικών σε ολόκληρη την εσωτερική αγορά, η Επιτροπή μπορεί να εκδίδει κατευθυντήριες γραμμές σχετικά με τις εν λόγω διαδικασίες, με την επιφύλαξη των αρμοδιοτήτων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

(63) Όλες οι βασικές και οι σημαντικές οντότητες δυνάμει της παρούσας οδηγίας θα πρέπει να υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο παρέχουν τις υπηρεσίες τους. Εάν η οντότητα παρέχει υπηρεσίες σε περισσότερα του ενός κράτη μέλη, θα πρέπει να υπάγεται στη χωριστή και συντρέχουσα δικαιοδοσία καθενός από τα εν λόγω 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.

(64) Προκειμένου να ληφθεί υπόψη ο διασυνοριακός χαρακτήρας των υπηρεσιών και των δραστηριοτήτων των παρόχων υπηρεσιών DNS, των μητρώων ονομάτων TLD, των παρόχων δικτύου διανομής περιεχομένου, των παρόχων υπηρεσιών νεφοϋπολογιστικής, των παρόχων υπηρεσιών κέντρου δεδομένων και των παρόχων ψηφιακών υπηρεσιών, 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 αντίστοιχη 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 εγκαταστάσεων. Από αυτή την

[25] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ αιτιολογική σκέψη (14) βάσει της οποίας «ο παρών κανονισμός δεν καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, περιλαμβανομένων της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου».

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 κριτήριο αυτό δεν θα πρέπει να εξαρτάται από το αν τα δικτυακά και πληροφοριακά συστήματα 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 είναι ο τόπος όπου λαμβάνονται στην Ένωση οι αποφάσεις που σχετίζονται με τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας. Αυτό συνήθως αντιστοιχεί στον τόπο της κεντρικής διοίκησης των εταιρειών εντός της Ένωσης. Εάν οι αποφάσεις αυτές δεν λαμβάνονται εντός της Ένωσης, η κύρια εγκατάσταση θα πρέπει να θεωρείται ότι βρίσκεται στα κράτη μέλη όπου η οντότητα διαθέτει 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.

(65) Σε περιπτώσεις που πάροχος υπηρεσιών DNS, μητρώο ονομάτων TLD, πάροχος δικτύου διανομής περιεχομένου, πάροχος υπηρεσιών νεφοϋπολογιστικής, πάροχος υπηρεσιών κέντρου δεδομένων και πάροχος ψηφιακών υπηρεσιών ο οποίος δεν είναι εγκατεστημένος στην Ένωση προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να ορίσει εκπρόσωπο. Για να προσδιοριστεί κατά πόσον μια τέτοια οντότητα προσφέρει υπηρεσίες εντός της Ένωσης, θα πρέπει να εξακριβώνεται αν είναι προφανές ότι η εν λόγω οντότητα σκοπεύει να προσφέρει υπηρεσίες σε πρόσωπα σε ένα η περισσότερα κράτη μέλη. Η προσβασιμότητα εντός της Ένωσης του ιστοτόπου της οντότητας ή μεσάζοντα ή διεύθυνσης ηλεκτρονικού ταχυδρομείου και άλλων στοιχείων επικοινωνίας, ή η χρήση γλώσσας που χρησιμοποιείται γενικά στην τρίτη χώρα όπου είναι εγκατεστημένος ο πάροχος ψηφιακών υπηρεσιών δεν αρκούν από μόνες τους για να εξακριβωθεί τέτοια πρόθεση. Ωστόσο, άλλοι παράγοντες όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιείται γενικά σε ένα ή περισσότερα κράτη μέλη με δυνατότητα παραγγελίας υπηρεσιών σε αυτή την άλλη γλώσσα ή οι αναφορές σε καταναλωτές ή χρήστες που βρίσκονται στην Ένωση μπορούν να καθιστούν προφανή την πρόθεση της οντότητας 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 έρχονται σε επαφή με αυτόν. Ο εκπρόσωπος θα πρέπει να ορίζεται ρητώς με γραπτή εντολή της οντότητας να ενεργεί για λογαριασμό του τελευταίου όσον αφορά τις υποχρεώσεις του που απορρέουν από την παρούσα οδηγία, συμπεριλαμβανομένης της αναφοράς περιστατικών.

(66) Σε περίπτωση ανταλλαγής, αναφοράς ή με άλλο τρόπο κοινοποίησης πληροφοριών που θεωρούνται διαβαθμισμένες σύμφωνα με το εθνικό ή το ενωσιακό δίκαιο δυνάμει των διατάξεων της παρούσας οδηγίας, θα πρέπει να εφαρμόζονται οι αντίστοιχοι ειδικοί κανόνες για τον χειρισμό διαβαθμισμένων πληροφοριών.

(67) Καθώς οι κυβερνοαπειλές καθίστανται ολοένα και πιο πολύπλοκες και εξελιγμένες, η λήψη άρτιων μέτρων εντοπισμού και πρόληψης εξαρτώνται σε μεγάλο βαθμό από την τακτική ανταλλαγή πληροφοριών και στοιχείων μεταξύ των οντοτήτων σχετικά με τις απειλές και τα τρωτά σημεία. Η ανταλλαγή πληροφοριών συμβάλλει στην αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές, η οποία ενισχύει με τη σειρά της την ικανότητα των οντοτήτων να αποτρέπουν τη μετατροπή απειλών σε πραγματικά περιστατικά, ενώ παρέχει επίσης στις οντότητες τη δυνατότητα να περιορίζουν καλύτερα τις επιπτώσεις των περιστατικών και να εξασφαλίζουν την αποκατάστασή τους με αποτελεσματικότερο τρόπο. Ελλείψει καθοδήγησης σε επίπεδο Ένωσης,

φαίνεται ότι η παρεμπόδιση της ανταλλαγής στοιχείων αυτού του είδους οφείλεται σε διάφορους παράγοντες, κυρίως στην αβεβαιότητα ως προς τη συμβατότητα με τους κανόνες ανταγωνισμού και τους κανόνες περί ευθύνης.

(68) Οι οντότητες θα πρέπει να ενθαρρύνονται να αξιοποιούν συλλογικά τις επιμέρους γνώσεις και την πρακτική εμπειρία που διαθέτουν σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο, με σκοπό την ενίσχυση των ικανοτήτων τους ώστε να είναι σε θέση να αξιολογούν, να παρακολουθούν, να υπερασπίζονται και να αντιμετωπίζουν δεόντως κυβερνοαπειλές. Ως εκ τούτου, είναι αναγκαίο να καταστεί δυνατή η δημιουργία μηχανισμών εθελούσιας ανταλλαγής πληροφοριών σε επίπεδο Ένωσης. Για τον σκοπό αυτό, τα κράτη μέλη θα πρέπει να υποστηρίζουν ενεργά και να ενθαρρύνουν επίσης τις σχετικές οντότητες που δεν καλύπτονται από το πεδίο εφαρμογής της παρούσας οδηγίας να συμμετέχουν στους εν λόγω μηχανισμούς ανταλλαγής πληροφοριών. Οι εν λόγω μηχανισμοί θα πρέπει να εφαρμόζονται σε πλήρη συμμόρφωση με τους κανόνες ανταγωνισμού της Ένωσης, καθώς και με τους κανόνες του ενωσιακού δικαίου για την προστασία των δεδομένων.

(69) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι απολύτως αναγκαία και αναλογική για τους σκοπούς της προστασίας της δικτυακής και πληροφοριακής ασφάλειας από οντότητες, δημόσιες αρχές, CERT, CSIRT και παρόχους τεχνολογιών και υπηρεσιών ασφάλειας, θα πρέπει να συνιστά έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων, όπως αναφέρεται στον κανονισμό (ΕΕ) 2016/679. Στο πλαίσιο αυτό θα πρέπει να περιλαμβάνονται μέτρα σχετικά με την πρόληψη, τον εντοπισμό, την ανάλυση και την αντιμετώπιση περιστατικών, μέτρα για την ευαισθητοποίηση σχετικά με συγκεκριμένες κυβερνοαπειλές, την ανταλλαγή πληροφοριών στο πλαίσιο της αποκατάστασης τρωτών σημείων και της συντονισμένης γνωστοποίησης, καθώς και την εθελούσια ανταλλαγή πληροφοριών σχετικά με τα εν λόγω περιστατικά, και τις κυβερνοαπειλές και τα τρωτά σημεία, τους δείκτες συμβιβασμού, τις τακτικές, τις τεχνικές και τις διαδικασίες, τις ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και τα εργαλεία διαμόρφωσης. Τα μέτρα αυτά μπορεί να απαιτούν την επεξεργασία των ακόλουθων τύπων δεδομένων προσωπικού χαρακτήρα: διευθύνσεις IP, ενιαίους εντοπιστές πόρων (URL), ονόματα τομέα και διευθύνσεις ηλεκτρονικού ταχυδρομείου.

(70) Προκειμένου να ενισχυθούν οι εποπτικές εξουσίες και δράσεις που συμβάλλουν στη διασφάλιση της αποτελεσματικής συμμόρφωσης, η παρούσα οδηγία θα πρέπει να προβλέπει έναν ελάχιστο κατάλογο εποπτικών δράσεων και μέσων με τα οποία 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 οντότητες όσο και για τις αρμόδιες αρχές. Ως εκ τούτου, οι βασικές οντότητες θα πρέπει να υπόκεινται σε πλήρες καθεστώς εποπτείας (εκ των προτέρων και εκ των υστέρων), ενώ οι σημαντικές οντότητες θα πρέπει να υπόκεινται σε απλοποιημένο, μόνο εκ των υστέρων, εποπτικό καθεστώς. Για την τελευταία περίπτωση, αυτό σημαίνει ότι οι σημαντικές οντότητες δεν θα πρέπει να τεκμηριώνουν συστηματικά τη συμμόρφωση με τις απαιτήσεις διαχείρισης κινδύνων κυβερνοασφάλειας, ενώ οι αρμόδιες αρχές θα πρέπει να εφαρμόζουν μια εκ των υστέρων προσέγγιση αντίδρασης όσον αφορά την εποπτεία και, ως εκ τούτου, να μην έχουν γενική υποχρέωση εποπτείας των εν λόγω οντοτήτων.

(71) Προκειμένου να καταστεί αποτελεσματική η επιβολή της νομοθεσίας, θα πρέπει να καταρτιστεί ένας ελάχιστος κατάλογος διοικητικών κυρώσεων για παραβίαση των υποχρεώσεων διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της

κυβερνοασφάλειας που προβλέπονται από την παρούσα οδηγία, με τη θέσπιση σαφούς και συνεκτικού πλαισίου για τις εν λόγω κυρώσεις σε ολόκληρη την Ένωση. Θα πρέπει να λαμβάνονται δεόντως υπόψη η φύση, η σοβαρότητα και η διάρκεια της παράβασης, η πραγματική ζημία που προκλήθηκε ή οι ζημίες που προκλήθηκαν ή οι δυνητικές ζημίες που θα μπορούσαν να προκληθούν, ο εκ προθέσεως ή εξ αμελείας χαρακτήρας της παράβασης, τα μέτρα που ελήφθησαν για την πρόληψη ή τον μετριασμό της ζημίας ή/και των απωλειών που σημειώθηκαν, ο βαθμός ευθύνης ή τυχόν σχετικών προηγούμενων παραβάσεων, ο βαθμός συνεργασίας με την αρμόδια αρχή και κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο. Η επιβολή κυρώσεων, συμπεριλαμβανομένων των διοικητικών προστίμων, 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, συμπεριλαμβανομένης της πραγματικής δικαστικής προστασίας και της ορθής διαδικασίας.

(72) 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.

(73) Σε περίπτωση που τα διοικητικά πρόστιμα επιβάλλονται σε επιχείρηση, μια επιχείρηση θα πρέπει να νοείται επιχείρηση σύμφωνα με τα άρθρα 101 και 102 ΣΛΕΕ για τους σκοπούς αυτούς. Σε περίπτωση που τα διοικητικά πρόστιμα επιβάλλονται σε πρόσωπα που δεν είναι επιχειρήσεις, η εποπτική 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.

(74) 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.

(75) Όταν η παρούσα οδηγία δεν εναρμονίζει διοικητικές ποινές ή αν είναι αναγκαίο σε άλλες περιπτώσεις, λόγου χάρη σε περιπτώσεις σοβαρών παραβάσεων των υποχρεώσεων που ορίζονται στην παρούσα οδηγία, τα κράτη μέλη θα πρέπει να εφαρμόζουν ένα σύστημα αποτελεσματικών, αναλογικών και αποτρεπτικών ποινών. Η φύση των εν λόγω ποινών, ποινικών ή διοικητικών, θα πρέπει να προσδιορίζεται από το δίκαιο των κρατών μελών.

(76) Προκειμένου να ενισχυθεί περαιτέρω η αποτελεσματικότητα και η αποτρεπτικότητα των κυρώσεων που επιβάλλονται σε περίπτωση παράβασης των υποχρεώσεων που καθορίζονται δυνάμει της παρούσας οδηγίας, οι αρμόδιες αρχές θα πρέπει να έχουν την εξουσία να επιβάλλουν κυρώσεις που συνίστανται στην αναστολή πιστοποίησης ή εξουσιοδότησης όσον αφορά μέρος ή το σύνολο των υπηρεσιών που παρέχονται από βασική οντότητα και στην επιβολή προσωρινής απαγόρευσης της άσκησης διαχειριστικών καθηκόντων από φυσικό πρόσωπο. Δεδομένης της σοβαρότητας και του αντικτύπου τους στις δραστηριότητες των οντοτήτων και, τελικά, στους καταναλωτές τους, οι εν λόγω κυρώσεις θα πρέπει να επιβάλλονται μόνο αναλογικά

με τη σοβαρότητα της παράβασης και λαμβάνοντας υπόψη τις ειδικές περιστάσεις κάθε περίπτωσης, συμπεριλαμβανομένου του εκ προθέσεως ή εξ αμελείας χαρακτήρα της παράβασης, των μέτρων που λαμβάνονται για την πρόληψη ή τον μετριασμό της ζημίας ή/και των ζημιών που σημειώθηκαν. Οι κυρώσεις αυτές θα πρέπει να επιβάλλονται μόνο ως ultima ratio, δηλαδή μόνο μετά την εξάντληση των άλλων σχετικών μέτρων επιβολής που προβλέπονται στην παρούσα οδηγία, και μόνο για το χρονικό διάστημα έως ότου οι οντότητες στις οποίες εφαρμόζονται λάβουν τα αναγκαία μέτρα για να συμπληρωθούν οι ελλείψεις ή για τη συμμόρφωση με τις απαιτήσεις της αρμόδιας αρχής για την οποία επιβλήθηκαν οι εν λόγω κυρώσεις. Η επιβολή των εν λόγω κυρώσεων, 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, συμπεριλαμβανομένης της αποτελεσματικής δικαστικής προστασίας, της ορθής διαδικασίας, του τεκμηρίου αθωότητας και του δικαιώματος της υπεράσπισης.

(77) Η παρούσα οδηγία θα πρέπει να θεσπίσει κανόνες συνεργασίας μεταξύ των αρμόδιων αρχών και των εποπτικών αρχών σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 για την αντιμετώπιση παραβάσεων που σχετίζονται με δεδομένα προσωπικού χαρακτήρα.

(78) Η παρούσα οδηγία θα πρέπει να αποσκοπεί στη διασφάλιση υψηλού επιπέδου ευθύνης για τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών σε επίπεδο οργανισμών. Για τους λόγους αυτούς, τα διοικητικά όργανα των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας θα πρέπει να εγκρίνουν τα μέτρα κινδύνου για την κυβερνοασφάλεια και να εποπτεύουν την εφαρμογή τους.

(79) Θα πρέπει να θεσπιστεί μηχανισμός αξιολόγησης από ομοτίμους, ο οποίος θα επιτρέπει την αξιολόγηση, από εμπειρογνώμονες που ορίζονται από τα κράτη μέλη, της εφαρμογής των πολιτικών κυβερνοασφάλειας, συμπεριλαμβανομένου του επιπέδου των ικανοτήτων και των διαθέσιμων πόρων των κρατών μελών.

(80) Προκειμένου να λαμβάνονται υπόψη οι νέες κυβερνοαπειλές, οι τεχνολογικές εξελίξεις ή οι τομεακές ιδιαιτερότητες, θα πρέπει να ανατεθεί στην Επιτροπή η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της ΣΛΕΕ όσον αφορά τα στοιχεία που αφορούν τα μέτρα διαχείρισης κινδύνου που απαιτούνται από την παρούσα οδηγία. Η Επιτροπή θα πρέπει επίσης να εξουσιοδοτηθεί να εκδίδει κατ' εξουσιοδότηση πράξεις για τον καθορισμό των κατηγοριών βασικών οντοτήτων που πρέπει να λαμβάνουν πιστοποιητικό και βάσει ποιων συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της 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[26]. Πιο συγκεκριμένα, προκειμένου να εξασφαλιστεί 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.

[26] ΕΕ L 123 της 12.5.2016, σ. 1.

(81) Προκειμένου να εξασφαλιστούν ενιαίοι όροι για την εφαρμογή των σχετικών διατάξεων της παρούσας οδηγίας σχετικά με τις διαδικαστικές ρυθμίσεις που απαιτούνται για τη λειτουργία της ομάδας συνεργασίας, τα τεχνικά στοιχεία που σχετίζονται με τα μέτρα διαχείρισης του κινδύνου ή το είδος των πληροφοριών, τη μορφή και τη διαδικασία των κοινοποιήσεων περιστατικών, θα πρέπει να ανατεθούν εκτελεστικές αρμοδιότητες στην Επιτροπή Οι εν λόγω αρμοδιότητες θα πρέπει να ασκούνται σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 182/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[27].

(82) Η Επιτροπή θα πρέπει να επανεξετάζει περιοδικά την παρούσα οδηγία, σε διαβούλευση με τα ενδιαφερόμενα μέρη, ιδίως προκειμένου να εξακριβώνεται αν απαιτείται τροποποίησή της υπό το πρίσμα της μεταβολής συνθηκών στην κοινωνία, την πολιτική, την τεχνολογία ή τις αγορές.

(83) Δεδομένου ότι ο στόχος της παρούσας οδηγίας, ήτοι η επίτευξη υψηλού ενιαίου επιπέδου κυβερνοασφάλειας στην 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.

(84) Η παρούσα οδηγία σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ιδιαίτερα δε το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την επιχειρηματική ελευθερία, το δικαίωμα ιδιοκτησίας, το δικαίωμα πραγματικής προσφυγής ενώπιον δικαστηρίου και το δικαίωμα ακρόασης. Η παρούσα οδηγία θα πρέπει να εφαρμόζεται σύμφωνα με τα δικαιώματα και τις αρχές αυτές,

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

ΚΕΦΑΛΑΙΟ Ι

Γενικές διατάξεις

Άρθρο 1

Αντικείμενο

1. Η παρούσα οδηγία θεσπίζει μέτρα με σκοπό τη διασφάλιση υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός της Ένωσης.

2. Για τον σκοπό αυτό, η οδηγία:

α) θεσπίζει υποχρεώσεις για τα κράτη μέλη όσον αφορά την έγκριση εθνικών στρατηγικών κυβερνοασφάλειας, τον ορισμό αρμόδιων εθνικών

[27] 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).

αρχών, ενιαίων σημείων επαφής και ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT)·

β) καθορίζει τις υποχρεώσεις διαχείρισης κινδύνου και αναφοράς περιστατικών στον τομέα της κυβερνοασφάλειας για οντότητα είδους που αναφέρεται ως βασική οντότητα στο παράρτημα Ι και ως σημαντική οντότητα στο παράρτημα ΙΙ·

γ) θεσπίζει υποχρεώσεις σχετικά με την ανταλλαγή πληροφοριών για την κυβερνοασφάλεια.

Άρθρο 2

Πεδίο εφαρμογής

1. Η παρούσα οδηγία εφαρμόζεται σε δημόσια ή ιδιωτική οντότητα είδους αναφερόμενου ως βασική οντότητα στο παράρτημα Ι και ως σημαντική οντότητα στο παράρτημα ΙΙ. Η παρούσα οδηγία δεν εφαρμόζεται σε οντότητες που χαρακτηρίζονται ως πολύ μικρές και μικρές επιχειρήσεις κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής.[28]

2. Ωστόσο, ανεξάρτητα από το μέγεθός τους, η παρούσα οδηγία εφαρμόζεται επίσης στις οντότητες που αναφέρονται στα παραρτήματα Ι και ΙΙ, εφόσον:

α) οι υπηρεσίες παρέχονται από μία από τις ακόλουθες οντότητες:

i) δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών που αναφέρονται στο παράρτημα Ι σημείο 8·

ii) παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο παράρτημα Ι σημείο 8·

iii) μητρώα ονομάτων τομέα ανωτάτου επιπέδου και παρόχου υπηρεσιών του συστήματος ονομάτων τομέα (DNS) που αναφέρονται στο παράρτημα Ι σημείο 8·

β) η οντότητα είναι φορέας δημόσιας διοίκησης όπως ορίζεται στο άρθρο 4 σημείο 23·

γ) η οντότητα είναι ο μοναδικός πάροχος υπηρεσίας σε κράτος μέλος·

δ) η ενδεχόμενη διατάραξη της υπηρεσίας που παρέχει η οντότητα θα μπορούσε να έχει επιπτώσεις στη δημόσια ασφάλεια, στη δημόσια προστασία ή στη δημόσια υγεία·

ε) ενδεχόμενη διατάραξη της υπηρεσίας που παρέχεται από την οντότητα θα μπορούσε να προκαλέσει συστημικούς κινδύνους, ιδίως για τους τομείς στους οποίους η διαταραχή αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο·

[28] 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).

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

ζ) η οντότητα χαρακτηρίζεται ως κρίσιμη οντότητα σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[29] [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] ή ως οντότητα ισοδύναμη με κρίσιμη οντότητα, σύμφωνα με το άρθρο 7 της εν λόγω οδηγίας.

Τα κράτη μέλη καταρτίζουν κατάλογο των οντοτήτων που προσδιορίζονται σύμφωνα με τα στοιχεία β) έως στ) και τον υποβάλλουν στην Επιτροπή έως τις [6 μήνες μετά την προθεσμία μεταφοράς στο εθνικό δίκαιο]. Σε τακτική βάση και τουλάχιστον ανά διετία, τα κράτη μέλη επανεξετάζουν και, εφόσον απαιτείται, επικαιροποιούν τον κατάλογο.

3. Η παρούσα οδηγία δεν θίγει τις αρμοδιότητες των κρατών μελών όσον αφορά τη διατήρηση της δημόσιας ασφάλειας, της άμυνας και της εθνικής ασφάλειας, σύμφωνα με το δίκαιο της Ένωσης.

4. Η παρούσα οδηγία εφαρμόζεται με την επιφύλαξη της οδηγίας 2008/114/ΕΚ του Συμβουλίου[30] και των οδηγιών 2011/93/ΕΕ[31] και 2013/40/ΕΕ[32] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

5. Με την επιφύλαξη του άρθρου 346 της ΣΛΕΕ, πληροφορίες που είναι εμπιστευτικές σύμφωνα με ενωσιακούς και εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές 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 βασικών ή σημαντικών οντοτήτων.

6. Όταν οι διατάξεις των τομεακών πράξεων του ενωσιακού δικαίου απαιτούν από βασικές ή σημαντικές οντότητες είτε να θεσπίζουν μέτρα διαχείρισης κινδύνου για την κυβερνοασφάλεια είτε να κοινοποιούν περιστατικά ή σημαντικές κυβερνοαπειλές, και εφόσον οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, δεν εφαρμόζονται οι σχετικές διατάξεις της παρούσας οδηγίας, συμπεριλαμβανομένης της διάταξης περί εποπτείας και επιβολής που προβλέπεται στο κεφάλαιο VI.

---

29 *[να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]*

30 Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους (ΕΕ L 345 της 23.12.2008, σ. 75).

31 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).

32 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).

Άρθρο 3

Ελάχιστη εναρμόνιση

Με την επιφύλαξη των λοιπών υποχρεώσεών τους βάσει του δικαίου της Ένωσης, τα κράτη μέλη μπορούν, σύμφωνα με την παρούσα οδηγία, να θεσπίζουν ή να διατηρούν διατάξεις που διασφαλίζουν υψηλότερο επίπεδο κυβερνοασφάλειας.

Άρθρο 4

Ορισμοί

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

1) «δικτυακό και πληροφοριακό σύστημα»:

   α) δίκτυο ηλεκτρονικών επικοινωνιών κατά την έννοια του άρθρου 2 σημείο 1) της οδηγίας (ΕΕ) 2018/1972,

   β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων,

   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 δικτυακών και πληροφοριακών συστημάτων»: η ικανότητα των δικτυακών και πληροφοριακών συστημάτων να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω δικτυακών και πληροφοριακών συστημάτων·

3) «κυβερνοασφάλεια»: κυβερνοασφάλεια κατά την έννοια του άρθρου 2 σημείο 1) του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[33]·

4) «εθνική στρατηγική κυβερνοασφάλειας»: συνεκτικό πλαίσιο κράτους μέλους το οποίο προβλέπει στρατηγικούς στόχους και προτεραιότητες για την ασφάλεια δικτυακών και πληροφοριακών συστημάτων στο εν λόγω κράτος μέλος·

5) «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 συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω δικτυακών και πληροφοριακών συστημάτων·

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

6) «χειρισμός περιστατικών»: όλες οι ενέργειες και διαδικασίες που αποσκοπούν στον εντοπισμό, την ανάλυση και την ανάσχεση ενός περιστατικού και στην αντιμετώπισή του·

7) «κυβερνοαπειλή»: κυβερνοαπειλή κατά την έννοια του άρθρου 2 σημείο 8 του κανονισμού (ΕΕ) 2019/881·

8) «τρωτό σημείο»: αδυναμία, ευαισθησία ή ελάττωμα πάγιου στοιχείου, συστήματος, διαδικασίας ή ελέγχου που μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης από κυβερνοαπειλή·

9) «εκπρόσωπος»: κάθε φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση που έχει οριστεί ρητά για να ενεργεί για λογαριασμό i) παρόχου υπηρεσιών DNS, μητρώου ονομάτων τομέα ανωτάτου επιπέδου (TLD), παρόχου υπηρεσιών νεφοϋπολογιστικής, παρόχου υπηρεσιών κέντρου δεδομένων, παρόχου δικτύου διανομής περιεχομένου όπως αναφέρεται στο παράρτημα I σημείο 8 ή ii) των οντοτήτων που αναφέρονται στο παράρτημα II σημείο 6 οι οποίες δεν είναι εγκατεστημένες στην Ένωση, στο οποίο μπορούν να απευθύνονται οι εθνικές αρμόδιες αρχές ή τα CSIRT αντί για την οντότητα όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας δυνάμει της παρούσας οδηγίας·

10) «πρότυπο»: πρότυπο κατά την έννοια του άρθρου 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[34]·

11) «τεχνική προδιαγραφή»: τεχνική προδιαγραφή κατά την έννοια του άρθρου 2 σημείο 4) του κανονισμού (ΕΕ) αριθ. 1025/2012·

12) «σημείο ανταλλαγής κίνησης διαδικτύου (Internet Exchange Point — IXP)»: δικτυακή υποδομή που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων δικτύων (αυτόνομων συστημάτων), κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης διαδικτύου και η οποία διασυνδέει μόνον αυτόνομα συστήματα· το IXP δεν απαιτεί η κίνηση διαδικτύου που διέρχεται μεταξύ οποιουδήποτε ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέλθει από τρίτο αυτόνομο σύστημα ούτε την τροποποιεί ούτε παρεμβαίνει με άλλον τρόπο σε αυτήν·

13) «σύστημα ονομάτων τομέα (DNS)»: ιεραρχικό και κατανεμημένο σύστημα ονοματοδοσίας το οποίο παρέχει στους τελικούς χρήστες πρόσβαση σε υπηρεσίες και πόρους του διαδικτύου·

14) «πάροχος υπηρεσιών DNS»: οντότητα που παρέχει υπηρεσίες αναδρομικής ή αυθεντικής επίλυσης ονομάτων τομέα σε τελικούς χρήστες του διαδικτύου και σε άλλους παρόχους υπηρεσιών DNS·

15) «μητρώο ονομάτων τομέα ανωτάτου επιπέδου»: οντότητα στην οποία έχει ανατεθεί συγκεκριμένος τομέας ανωτάτου επιπέδου (TLD) και η οποία είναι υπεύθυνη για τη διοίκηση του TLD, συμπεριλαμβανομένης της καταχώρισης ονομάτων τομέα στον TLD και της τεχνικής λειτουργίας του, στην οποία περιλαμβάνεται η λειτουργία των

[34] 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).

εξυπηρετητών ονομάτων του, η συντήρηση των βάσεων δεδομένων του και η κατανομή των αρχείων ζώνης TLD μεταξύ των εξυπηρετητών ονομάτων·

16) «ψηφιακή υπηρεσία»: υπηρεσία κατά την έννοια του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[35]·

17) «επιγραμμική αγορά»: ψηφιακή υπηρεσία κατά την έννοια του άρθρου 2 στοιχείο ιδ) της οδηγίας 2005/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[36]·

18) «επιγραμμική μηχανή αναζήτησης»: ψηφιακή υπηρεσία κατά την έννοια του άρθρου 2 σημείο 5) του κανονισμού (ΕΕ) 2019/1150 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[37]·

19) «υπηρεσία νεφοϋπολογιστικής»: ψηφιακή υπηρεσία που επιτρέπει κατά παραγγελία διαχείριση και ευρεία εξ αποστάσεως πρόσβαση σε κλιμακούμενο και ελαστικό σύνολο κοινόχρηστων και κατανεμημένων υπολογιστικών πόρων.

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

21) «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·

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

23) «φορέας δημόσιας διοίκησης»: οντότητα κράτους μέλους που 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·

γ) χρηματοδοτείται κατά το μεγαλύτερο μέρος από το κράτος, περιφερειακές αρχές ή άλλους οργανισμούς δημοσίου δικαίου ή η διαχείρισή του υπόκειται στην εποπτεία των εν λόγω αρχών ή των εν λόγω οργανισμών ή έχει

---

35 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).

36 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).

37 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).

διοικητικό, διευθυντικό ή εποπτικό συμβούλιο, του οποίου περισσότερα από τα μισά μέλη διορίζονται από τις κρατικές ή περιφερειακές αρχές ή από άλλους οργανισμούς δημοσίου δικαίου·

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

Εξαιρούνται οι φορείς δημόσιας διοίκησης που εκτελούν δραστηριότητες στους τομείς της δημόσιας ασφάλειας, της επιβολής του νόμου, της άμυνας ή της εθνικής ασφάλειας.

24) «οντότητα »: κάθε φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο σύμφωνα με το εθνικό δίκαιο του τόπου εγκατάστασής του, το οποίο μπορεί, ενεργώντας εξ ιδίου ονόματος, να ασκεί δικαιώματα και να αναλαμβάνει υποχρεώσεις·

25) «βασική οντότητα»: κάθε οντότητα τύπου που αναφέρεται ως βασική οντότητα στο παράρτημα Ι·

26) «σημαντική οντότητα»: κάθε οντότητα τύπου που αναφέρεται ως σημαντική οντότητα στο παράρτημα ΙΙ.

ΚΕΦΑΛΑΙΟ ΙΙ

Συντονισμένα κανονιστικά πλαίσια κυβερνοασφάλειας

Άρθρο 5

Εθνική στρατηγική κυβερνοασφάλειας

1. Κάθε κράτος μέλος θεσπίζει εθνική στρατηγική κυβερνοασφάλειας, η οποία καθορίζει τους στρατηγικούς στόχους και κατάλληλα μέτρα πολιτικής και κανονιστικά μέτρα, με σκοπό την επίτευξη και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας. Η εθνική στρατηγική κυβερνοασφάλειας περιλαμβάνει, συγκεκριμένα, τα εξής:

α) ορισμό των στόχων και των προτεραιοτήτων της στρατηγικής των κρατών μελών στον τομέα της κυβερνοασφάλειας·

β) πλαίσιο διακυβέρνησης για την επίτευξη των εν λόγω στόχων και προτεραιοτήτων, συμπεριλαμβανομένων των πολιτικών που αναφέρονται στην παράγραφο 2 και των ρόλων και των αρμοδιοτήτων των δημόσιων φορέων και οντοτήτων, καθώς και άλλων σχετικών φορέων·

γ) αξιολόγηση για τον προσδιορισμό των σχετικών πάγιων στοιχείων και των κινδύνων για την κυβερνοασφάλεια στο εν λόγω κράτος μέλος·

δ) προσδιορισμό των μέτρων που διασφαλίζουν την ετοιμότητα για περιστατικά, την αντιμετώπισή τους και την αποκατάσταση των συστημάτων, συμπεριλαμβανομένης της συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα·

ε) κατάλογο των διαφόρων αρχών και φορέων που συμμετέχουν στην εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας·

στ) πλαίσιο πολιτικής για την ενίσχυση του συντονισμού μεταξύ των αρμόδιων αρχών δυνάμει της παρούσας οδηγίας και της οδηγίας (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[38] [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] με σκοπό την ανταλλαγή πληροφοριών σχετικά με περιστατικά και κυβερνοαπειλές και την άσκηση εποπτικών καθηκόντων.

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

α) πολιτική σχετικά με την κυβερνοασφάλεια στην αλυσίδα εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ που χρησιμοποιούνται από βασικές και σημαντικές οντότητες για την παροχή των υπηρεσιών τους·

β) κατευθυντήριες γραμμές σχετικά με τη συμπερίληψη και τον προσδιορισμό απαιτήσεων σχετικών με την κυβερνοασφάλεια όσον αφορά προϊόντα και υπηρεσίες ΤΠΕ στις δημόσιες συμβάσεις·

γ) πολιτική για την προώθηση και τη διευκόλυνση της συντονισμένης γνωστοποίησης τρωτών σημείων κατά την έννοια του άρθρου 6·

δ) πολιτική σχετικά με τη διατήρηση της γενικής διαθεσιμότητας και ακεραιότητας του δημόσιου πυρήνα του ανοικτού διαδικτύου·

ε) πολιτική για την προώθηση και την ανάπτυξη δεξιοτήτων, δραστηριοτήτων ευαισθητοποίησης και πρωτοβουλιών έρευνας και ανάπτυξης στον τομέα της κυβερνοασφάλειας·

στ) πολιτική για τη στήριξη των πανεπιστημιακών και ερευνητικών ιδρυμάτων με σκοπό την ανάπτυξη εργαλείων κυβερνοασφάλειας και ασφαλών δικτυακών υποδομών·

ζ) πολιτική, σχετικές διαδικασίες και κατάλληλα εργαλεία ανταλλαγής πληροφοριών για τη στήριξη της εθελούσιας ανταλλαγής πληροφοριών σχετικά με την κυβερνοασφάλεια μεταξύ εταιρειών σύμφωνα με το δίκαιο της Ένωσης·

η) πολιτική για την αντιμετώπιση ειδικών αναγκών των ΜΜΕ, ιδίως εκείνων που εξαιρούνται από το πεδίο εφαρμογής της παρούσας οδηγίας, όσον αφορά την καθοδήγηση και τη στήριξή τους για τη βελτίωση της ανθεκτικότητάς τους έναντι απειλών κυβερνοασφάλειας.

3. Τα κράτη μέλη κοινοποιούν τις εθνικές στρατηγικές κυβερνοασφάλειας στην Επιτροπή εντός τριών μηνών από την έγκρισή τους. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες πληροφορίες από την κοινοποίηση στις περιπτώσεις και στον βαθμό που είναι απολύτως αναγκαίο για την προστασία της εθνικής ασφάλειας.

4. Τα κράτη μέλη αξιολογούν τις εθνικές στρατηγικές κυβερνοασφάλειας τουλάχιστον ανά τετραετία με βάση βασικούς δείκτες επιδόσεων και τις τροποποιούν αν κρίνεται απαραίτητο. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) επικουρεί τα κράτη μέλη, κατόπιν αιτήματος, στην ανάπτυξη εθνικής στρατηγικής και βασικών δεικτών επιδόσεων για την αξιολόγηση της στρατηγικής τους.

[38] *[να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]*

Άρθρο 6

Συντονισμένη γνωστοποίηση τρωτών σημείων και ευρωπαϊκό μητρώο τρωτών σημείων

1. Κάθε κράτος μέλος ορίζει μία από τις CSIRT του, οι οποίες αναφέρονται στο άρθρο 9, ως συντονίστρια για τον σκοπό της συντονισμένης γνωστοποίησης τρωτών σημείων. Η ορισθείσα CSIRT ενεργεί ως αξιόπιστος ενδιάμεσος φορέας, διευκολύνοντας, αν είναι αναγκαίο, την επικοινωνία μεταξύ της αναφέρουσας οντότητας και του κατασκευαστή ή του παρόχου προϊόντων ή υπηρεσιών ΤΠΕ. Όταν το αναφερόμενο τρωτό σημείο αφορά πολλαπλούς κατασκευαστές ή παρόχους προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ σε ολόκληρη την Ένωση, η ορισθείσα CSIRT κάθε ενδιαφερόμενου κράτους μέλους συνεργάζεται με το δίκτυο CSIRT.

2. Ο ENISA δημιουργεί και διατηρεί ευρωπαϊκό μητρώο τρωτών σημείων. Για τον σκοπό αυτό, ο ENISA δημιουργεί και διατηρεί κατάλληλα πληροφοριακά συστήματα και κατάλληλες πολιτικές και διαδικασίες προκειμένου, ιδίως, να παρέχει τη δυνατότητα στις σημαντικές και στις βασικές οντότητες και στους προμηθευτές δικτυακών και πληροφοριακών συστημάτων τους να γνωστοποιούν και να καταγράφουν τρωτά σημεία που παρατηρούνται σε προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ, καθώς και να παρέχει πρόσβαση στις πληροφορίες σχετικά με τρωτά σημεία που περιλαμβάνονται στο μητρώο σε όλα τα ενδιαφερόμενα μέρη. Το μητρώο περιλαμβάνει, συγκεκριμένα, πληροφορίες που περιγράφουν το τρωτό σημείο, το προϊόν ΤΠΕ ή τις υπηρεσίες ΤΠΕ που επηρεάζονται και τη σοβαρότητα του τρωτού σημείου από την άποψη των περιστάσεων υπό τις οποίες μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης, τη διαθεσιμότητα σχετικών διορθωτικών προγραμμάτων και, ελλείψει διαθέσιμων διορθωτικών προγραμμάτων, υλικό καθοδήγησης που απευθύνεται στους χρήστες τρωτών προϊόντων και υπηρεσιών σχετικά με τον τρόπο μετριασμού των κινδύνων που απορρέουν από τα γνωστοποιημένα τρωτά σημεία.

Άρθρο 7

Εθνικά πλαίσια διαχείρισης κρίσεων κυβερνοασφάλειας

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν επαρκείς πόρους για την αποτελεσματική και αποδοτική εκτέλεση των καθηκόντων που τους ανατίθενται.

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

3. Κάθε κράτος μέλος θεσπίζει εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας, στο οποίο καθορίζονται στόχοι και λεπτομέρειες της διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας. Στο σχέδιο αυτό καθορίζονται, συγκεκριμένα, τα εξής:

   α) οι στόχοι των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας·

   β) τα καθήκοντα και οι αρμοδιότητες των εθνικών αρμόδιων αρχών·

γ) οι διαδικασίες διαχείρισης κρίσεων και οι δίαυλοι ανταλλαγής πληροφοριών·

δ) μέτρα ετοιμότητας, συμπεριλαμβανομένων ασκήσεων και δραστηριοτήτων κατάρτισης·

ε) τα συναφή ενδιαφερόμενα μέρη και οι υποδομές του δημόσιου και του ιδιωτικού τομέα·

στ) 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 και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας σε επίπεδο Ένωσης.

4. Τα κράτη μέλη κοινοποιούν στην Επιτροπή τον ορισμό των αρμόδιων αρχών που αναφέρονται στην παράγραφο 1 και υποβάλλουν τα εθνικά τους σχέδια αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας, τα οποία αναφέρονται στην παράγραφο 3, εντός τριών μηνών από τον ορισμό των εν λόγω αρχών και από την έγκριση των εν λόγω σχεδίων. Τα κράτη μέλη μπορούν να εξαιρούν συγκεκριμένες πληροφορίες από το σχέδιο στις περιπτώσεις και στον βαθμό που είναι απολύτως αναγκαίο για λόγους εθνικής ασφάλειας.

Άρθρο 8

Εθνικές αρμόδιες αρχές και ενιαία σημεία επαφής

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την κυβερνοασφάλεια και για τα εποπτικά καθήκοντα που αναφέρονται στο κεφάλαιο VI της παρούσας οδηγίας. Για τον σκοπό αυτόν, τα κράτη μέλη μπορούν να ορίσουν υφιστάμενη αρχή ή υφιστάμενες αρχές.

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

3. Κάθε κράτος μέλος ορίζει ένα εθνικό ενιαίο σημείο επαφής για θέματα κυβερνοασφάλειας («ενιαίο σημείο επαφής»). Εάν κάποιο κράτος μέλος ορίσει μόνο μία αρμόδια αρχή, η εν λόγω αρμόδια αρχή αποτελεί επίσης το ενιαίο σημείο επαφής του εν λόγω κράτους μέλους.

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

5. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές που αναφέρονται στην παράγραφο 1 και τα ενιαία σημεία επαφής διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους ανατίθενται και να επιτυγχάνουν, με τον τρόπο αυτό, τους στόχους της παρούσας οδηγίας. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των εκπροσώπων που ορίζουν στο πλαίσιο της ομάδας συνεργασίας που αναφέρεται στο άρθρο 12.

6. Κάθε κράτος μέλος κοινοποιεί στην Επιτροπή, χωρίς αδικαιολόγητη καθυστέρηση, τον ορισμό της αρμόδιας αρχής της παραγράφου 1 και του ενιαίου σημείου επαφής της παραγράφου 3, τα καθήκοντά τους καθώς και κάθε μεταγενέστερη τροποποίηση

των στοιχείων αυτών. Κάθε κράτος μέλος δημοσιοποιεί την αρμόδια αρχή και το ενιαίο σημείο επαφής που έχει ορίσει. Η Επιτροπή δημοσιεύει τον κατάλογο των ορισθέντων ενιαίων σημείων επαφής.

Άρθρο 9

Ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT)

1. Κάθε κράτος μέλος ορίζει μία ή περισσότερες CSIRT, οι οποίες συμμορφώνονται με τις απαιτήσεις που ορίζονται στο άρθρο 10 παράγραφος 1, καλύπτουν τουλάχιστον τους τομείς, τους επιμέρους τομείς ή τις οντότητες που αναφέρονται στα παραρτήματα Ι και ΙΙ, και είναι υπεύθυνες για τον χειρισμό περιστατικών βάσει σαφώς καθορισμένης διαδικασίας. Η CSIRT μπορεί να συσταθεί εντός της αρμόδιας αρχής που αναφέρεται στο άρθρο 8.
2. Τα κράτη μέλη εξασφαλίζουν ότι κάθε CSIRT διαθέτει επαρκείς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων της που περιγράφονται στο άρθρο 10 παράγραφος 2.
3. Τα κράτη μέλη διασφαλίζουν ότι κάθε CSIRT διαθέτει κατάλληλη, ασφαλή και ανθεκτική υποδομή επικοινωνίας και πληροφοριών για την ανταλλαγή πληροφοριών με βασικές και σημαντικές οντότητες και άλλα σχετικά ενδιαφερόμενα μέρη. Για τον σκοπό αυτόν, τα κράτη μέλη διασφαλίζουν ότι οι CSIRT συμβάλλουν στην εγκατάσταση ασφαλών εργαλείων ανταλλαγής πληροφοριών.
4. Οι CSIRT συνεργάζονται και, κατά περίπτωση, ανταλλάσσουν σχετικές πληροφορίες σύμφωνα με το άρθρο 26 με αξιόπιστες τομεακές ή διατομεακές κοινότητες βασικών και σημαντικών οντοτήτων.
5. Οι CSIRT συμμετέχουν σε αξιολογήσεις από ομοτίμους που διοργανώνονται σύμφωνα με το άρθρο 16.
6. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των CSIRT τους στο πλαίσιο του δικτύου CSIRT που αναφέρεται στο άρθρο 13.
7. Τα κράτη μέλη κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην Επιτροπή τις CSIRT που έχουν ορίσει σύμφωνα με την παράγραφο 1, τη συντονίστρια CSIRT που έχουν ορίσει σύμφωνα με το άρθρο 6 παράγραφος 1 και τα αντίστοιχα καθήκοντά τους σε σχέση με τις οντότητες που αναφέρονται στα παραρτήματα Ι και ΙΙ.
8. Τα κράτη μέλη μπορούν να ζητούν τη συνδρομή του ENISA για τη δημιουργία των εθνικών τους CSIRT.

Άρθρο 10

Απαιτήσεις και καθήκοντα των CSIRT

1. Οι CSIRT συμμορφώνονται με τις ακόλουθες απαιτήσεις:
   α) οι CSIRT εξασφαλίζουν υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών τους αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτουν διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. Οι CSIRT προσδιορίζουν σαφώς τους διαύλους επικοινωνίας

και τους γνωστοποιούν στα μέλη της περιοχής ευθύνης τους και στους συνεργαζόμενους εταίρους·

β) τα γραφεία των CSIRT και τα υποστηρικτικά πληροφοριακά συστήματα εγκαθίστανται σε ασφαλείς τοποθεσίες·

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 είναι επαρκώς στελεχωμένες ώστε να εξασφαλίζεται η διαθεσιμότητά τους ανά πάσα στιγμή,

ε) οι CSIRT είναι εξοπλισμένες με πλεονάζοντα συστήματα και εφεδρικό χώρο εργασίας, ώστε να εξασφαλίζεται η συνέχεια των υπηρεσιών τους·

στ) οι CSIRT έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας.

2. Οι CSIRT είναι επιφορτισμένες με τα ακόλουθα καθήκοντα:

α) παρακολούθηση των κυβερνοαπειλών, των τρωτών σημείων και των περιστατικών σε εθνικό επίπεδο·

β) παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων επαγρύπνησης και ανακοινώσεων και διάδοση πληροφοριών στις βασικές και στις σημαντικές οντότητες, καθώς και σε άλλα ενδιαφερόμενα μέρη σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά·

γ) αντιμετώπιση περιστατικών·

δ) παροχή δυναμικής ανάλυσης κινδύνων και περιστατικών και επίγνωση της κατάστασης σε θέματα κυβερνοασφάλειας·

ε) παροχή, κατόπιν αιτήματος της οντότητας, προληπτικής σάρωσης των δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιεί μια οντότητα για την παροχή των υπηρεσιών της·

στ) συμμετοχή στο δίκτυο CSIRT και παροχή αμοιβαίας συνδρομής σε άλλα μέλη του δικτύου κατόπιν αιτήματός τους.

3. Οι CSIRT αναπτύσσουν σχέσεις συνεργασίας με σχετικούς φορείς του ιδιωτικού τομέα, με σκοπό την καλύτερη επίτευξη των στόχων της οδηγίας.

4. Προκειμένου να διευκολύνουν τη συνεργασία, οι CSIRT προωθούν την έκδοση και χρήση κοινών ή τυποποιημένων πρακτικών, συστημάτων ταξινόμησης και ταξινομιών σε σχέση με τα ακόλουθα:

α) διαδικασίες χειρισμού περιστατικών·

β) τη διαχείριση κρίσεων κυβερνοασφάλειας·

γ) τη συντονισμένη γνωστοποίηση τρωτών σημείων.

Άρθρο 11
Συνεργασία σε εθνικό επίπεδο

1. Εφόσον πρόκειται για διακριτές οντότητες, οι αρμόδιες αρχές που αναφέρονται στο άρθρο 8, το ενιαίο σημείο επαφής και η/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 είτε οι αρμόδιες αρχές τους είτε οι CSIRT τους λαμβάνουν κοινοποιήσεις για περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που υποβάλλονται σύμφωνα με την παρούσα οδηγία. Αν ένα κράτος μέλος αποφασίσει ότι οι CSIRT του δεν θα λαμβάνουν τις εν λόγω κοινοποιήσεις, παρέχεται στις CSIRT, στον βαθμό που είναι αναγκαίος για την εκτέλεση των καθηκόντων τους, πρόσβαση σε δεδομένα σχετικά με περιστατικά που κοινοποιούνται από τις βασικές ή τις σημαντικές οντότητες, σύμφωνα με το άρθρο 20.

3. Κάθε κράτος μέλος μεριμνά ώστε οι αρμόδιες αρχές ή οι CSIRT του να ενημερώνουν το ενιαίο σημείο επαφής του για κοινοποιήσεις σχετικά με περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που υποβάλλονται σύμφωνα με την παρούσα οδηγία.

4. Στον βαθμό που απαιτείται για την αποτελεσματική εκτέλεση των καθηκόντων και υποχρεώσεων που ορίζονται στην παρούσα οδηγία, τα κράτη μέλη μεριμνούν για την κατάλληλη συνεργασία μεταξύ των αρμόδιων αρχών και των ενιαίων σημείων επαφής, των αρχών επιβολής του νόμου, των αρχών προστασίας δεδομένων και των αρχών που είναι υπεύθυνες για τις κρίσιμες υποδομές σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων], καθώς και των εθνικών χρηματοπιστωτικών αρχών που ορίζονται σύμφωνα με τον κανονισμό (ΕΕ) XXXX/XXXX του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[39] [κανονισμός DORA] εντός του εν λόγω κράτους μέλους.

5. Τα κράτη μέλη μεριμνούν ώστε οι αρμόδιες αρχές τους να παρέχουν τακτικά πληροφορίες στις αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] σχετικά με τους κινδύνους κυβερνοασφάλειας, τις κυβερνοαπειλές και τα περιστατικά που επηρεάζουν βασικές οντότητες που έχουν χαρακτηριστεί κρίσιμες ή οντότητες ισοδύναμες με κρίσιμες οντότητες, σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων], καθώς και με τα μέτρα που λαμβάνουν οι αρμόδιες αρχές για την αντιμετώπιση των εν λόγω κινδύνων και περιστατικών.

ΚΕΦΑΛΑΙΟ III

Συνεργασία

Άρθρο 12
Ομάδα συνεργασίας

1. Συγκροτείται ομάδα συνεργασίας με σκοπό να υποστηριχθεί και να διευκολυνθεί η στρατηγική συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών εντός του πεδίου εφαρμογής της οδηγίας.

[39] *[να αναγραφεί ο πλήρης τίτλος και τα στοιχεία δημοσίευσης της ΕΕ όταν είναι γνωστά]*

2. Η ομάδα συνεργασίας εκτελεί τα καθήκοντά της βάσει διετών προγραμμάτων εργασιών τα οποία αναφέρονται στην παράγραφο 6.

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) σύμφωνα με το άρθρο 17 παράγραφος 5 στοιχείο γ) του κανονισμού (ΕΕ) XXXX/XXXX [κανονισμός DORA] μπορούν να συμμετέχουν στις δραστηριότητες της ομάδας συνεργασίας.

Ανάλογα με την περίπτωση, η ομάδα συνεργασίας μπορεί να καλεί εκπροσώπους σχετικών ενδιαφερόμενων φορέων 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) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σχετικά με την εφαρμογή της παρούσας οδηγίας, μεταξύ άλλων όσον αφορά κυβερνοαπειλές, περιστατικά, τρωτά σημεία, παρ' ολίγον περιστατικά, πρωτοβουλίες ευαισθητοποίησης, προγράμματα κατάρτισης, ασκήσεις και δεξιότητες, ανάπτυξη ικανοτήτων, καθώς και πρότυπα και τεχνικές προδιαγραφές·

γ) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με αναδυόμενες πρωτοβουλίες πολιτικής σε θέματα κυβερνοασφάλειας·

δ) ανταλλαγή συμβουλών και συνεργασία με την Επιτροπή σχετικά με σχέδια εκτελεστικών ή κατ' εξουσιοδότηση πράξεων της Επιτροπής που εκδίδονται δυνάμει της παρούσας οδηγίας·

ε) ανταλλαγή βέλτιστων πρακτικών και πληροφοριών με τα σχετικά θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης·

στ) συζήτηση των εκθέσεων σχετικά με την αξιολόγηση από ομοτίμους που αναφέρεται στο άρθρο 16 παράγραφος 7·

ζ) συζήτηση των αποτελεσμάτων κοινών εποπτικών δραστηριοτήτων σε διασυνοριακές υποθέσεις, όπως αναφέρεται στο άρθρο 34·

η) παροχή στρατηγικής καθοδήγησης στο δίκτυο CSIRT σχετικά με συγκεκριμένα αναδυόμενα ζητήματα·

θ) συνεισφορά στις ικανότητες κυβερνοασφάλειας όλων των χωρών της Ένωσης με τη διευκόλυνση της ανταλλαγής εθνικών υπαλλήλων μέσω προγράμματος ανάπτυξης ικανοτήτων με τη συμμετοχή προσωπικού από τις αρμόδιες αρχές ή τις CSIRT των κρατών μελών·

ι) διοργάνωση τακτικών κοινών συνεδριάσεων με σχετικούς ιδιωτικούς ενδιαφερόμενους φορείς από ολόκληρη την Ένωση για τη συζήτηση των δραστηριοτήτων που πραγματοποιεί η ομάδα και τη συγκέντρωση στοιχείων σχετικά με αναδυόμενες προκλήσεις πολιτικής·

ια) συζήτηση των εργασιών που σχετίζονται με τις ασκήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων των εργασιών που εκτελεί ο ENISA.

5. Η ομάδα συνεργασίας μπορεί να ζητήσει από το δίκτυο CSIRT να εκπονήσει τεχνική έκθεση σχετικά με επιλεγμένα θέματα.

6. Έως ... [24 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας] και ανά διετία στη συνέχεια, η ομάδα συνεργασίας καταρτίζει πρόγραμμα εργασιών σχετικά με τις δράσεις που πρέπει να αναληφθούν για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα του πρώτου προγράμματος που θα εγκριθεί δυνάμει της παρούσας οδηγίας ευθυγραμμίζεται με το χρονοδιάγραμμα του τελευταίου προγράμματος που εγκρίθηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148.

7. 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 που αναφέρεται στο άρθρο 37 παράγραφος 2.

8. Η ομάδα συνεργασίας συνεδριάζει τακτικά και τουλάχιστον μία φορά ετησίως με την ομάδα ανθεκτικότητας κρίσιμων οντοτήτων που συστάθηκε βάσει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων] με σκοπό την προώθηση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών.

Άρθρο 13
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 των κρατών μελών και της CERT-EU. Η Επιτροπή συμμετέχει στο δίκτυο CSIRT ως παρατηρητής. Ο ENISA παρέχει τη γραμματειακή υποστήριξη και υποστηρίζει ενεργά τη συνεργασία μεταξύ των CSIRT.

3. Τα καθήκοντα του δικτύου CSIRT είναι τα εξής:

   α) ανταλλαγή πληροφοριών σχετικά με τις ικανότητες των CSIRT·

   β) ανταλλαγή σημαντικών πληροφοριών σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και τρωτά σημεία·

   γ) κατόπιν αιτήματος εκπροσώπου του δικτύου CSIRT που έχει ενδεχομένως επηρεαστεί από περιστατικό, ανταλλαγή και συζήτηση πληροφοριών σχετικά με το εν λόγω περιστατικό και τις συναφείς κυβερνοαπειλές, τους κινδύνους και τα τρωτά σημεία·

   δ) κατόπιν αιτήματος εκπροσώπου του δικτύου CSIRT, συζήτηση και, αν είναι δυνατόν, εφαρμογή συντονισμένης αντιμετώπισης περιστατικού που έχει διαπιστωθεί εντός της δικαιοδοσίας του συγκεκριμένου κράτους μέλους·

   ε) παροχή στήριξης στα κράτη μέλη για την αντιμετώπιση διασυνοριακών περιστατικών σύμφωνα με την παρούσα οδηγία·

   στ) συνεργασία και παροχή συνδρομής στις ορισθείσες CSIRT που αναφέρονται στο άρθρο 6 όσον αφορά τη διαχείριση της πολυμερούς συντονισμένης γνωστοποίησης τρωτών σημείων που επηρεάζουν πολλαπλούς κατασκευαστές

ή παρόχους προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που είναι εγκατεστημένοι σε διαφορετικά κράτη μέλη·

ζ) συζήτηση και προσδιορισμός περαιτέρω μορφών επιχειρησιακής συνεργασίας, μεταξύ άλλων όσον αφορά:

i) τις κατηγορίες κυβερνοαπειλών και περιστατικών·

ii) τις έγκαιρες προειδοποιήσεις·

iii) την αμοιβαία συνδρομή·

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

v) τη συμβολή στο εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας που αναφέρεται στο άρθρο 7 παράγραφος 3·

η) ενημέρωση της ομάδας συνεργασίας σχετικά με τις δραστηριότητές του και τις περαιτέρω μορφές επιχειρησιακής συνεργασίας που συζητούνται σύμφωνα με το στοιχείο ζ), και, στις περιπτώσεις που κρίνεται απαραίτητο, υποβολή σχετικού αιτήματος καθοδήγησης·

θ) άντληση διδαγμάτων από ασκήσεις κυβερνοασφάλειας, μεταξύ άλλων από τις ασκήσεις που διοργανώνει ο ENISA·

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

ια) 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 απειλές σε ολόκληρη την Ένωση·

ιβ) συζήτηση των εκθέσεων αξιολόγησης από ομοτίμους που αναφέρονται στο άρθρο 16 παράγραφος 7·

ιγ) έκδοση 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. Για τους σκοπούς της επανεξέτασης που αναφέρεται στο άρθρο 35 και έως [24 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας], και ανά διετία στη συνέχεια, το δίκτυο CSIRT αξιολογεί την πρόοδο που έχει σημειωθεί στον τομέα της επιχειρησιακής συνεργασίας και συντάσσει σχετική έκθεση. Ειδικότερα, στην έκθεση συνάγονται συμπεράσματα σχετικά με τα αποτελέσματα των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 16, οι οποίες διενεργούνται σχετικά με τις εθνικές CSIRT, συμπεριλαμβανομένων συμπερασμάτων και συστάσεων, δυνάμει του εν λόγω άρθρου. Η εν λόγω έκθεση υποβάλλεται επίσης στην ομάδα συνεργασίας.

5. Το δίκτυο CSIRT εγκρίνει τον εσωτερικό του κανονισμό.

Άρθρο 14

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

1. Δημιουργείται το ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU - CyCLONe) με σκοπό τη στήριξη της συντονισμένης διαχείρισης περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας σε επιχειρησιακό επίπεδο και τη διασφάλιση της τακτικής ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

2. Το δίκτυο EU-CyCLONe απαρτίζεται από τους εκπροσώπους των αρχών διαχείρισης κρίσεων των κρατών μελών που ορίζονται σύμφωνα με το άρθρο 7, της Επιτροπής και του ENISA. Ο ENISA παρέχει γραμματειακή υποστήριξη στο δίκτυο και υποστηρίζει την ασφαλή ανταλλαγή πληροφοριών.

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

   α) αύξηση του επιπέδου ετοιμότητας για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας·

   β) ανάπτυξη κοινής επίγνωσης της κατάστασης όσον αφορά σημαντικά συμβάντα κυβερνοασφάλειας·

   γ) συντονισμός της διαχείρισης περιστατικών και κρίσεων μεγάλης κλίμακας και υποστήριξη της λήψης αποφάσεων σε πολιτικό επίπεδο όσον αφορά τα εν λόγω περιστατικά και τις κρίσεις·

   δ) συζήτηση των εθνικών σχεδίων αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας που αναφέρονται στο άρθρο 7 παράγραφος 2·

4. Το EU-CyCLONe εγκρίνει τον εσωτερικό κανονισμό του.

5. Το EU-CyCLONe υποβάλλει τακτικά εκθέσεις στην ομάδα συνεργασίας σχετικά με τις απειλές, τα περιστατικά και τις τάσεις στον κυβερνοχώρο, εστιάζοντας ιδίως στον αντίκτυπό τους στις βασικές και τις σημαντικές οντότητες.

6. Το EU-CyCLONe συνεργάζεται με το δίκτυο CSIRT βάσει συμφωνημένων διαδικαστικών ρυθμίσεων.

Άρθρο 15

Έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση

1. Ο ENISA εκδίδει, σε συνεργασία με την Επιτροπή, έκθεση ανά διετία σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση. Συγκεκριμένα, στην έκθεση αξιολογούνται, μεταξύ άλλων, τα εξής:

   α) η ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση·

   β) οι τεχνικοί, οικονομικοί και ανθρώπινοι πόροι που διατίθενται στις αρμόδιες αρχές και στις πολιτικές κυβερνοασφάλειας, καθώς και η εφαρμογή εποπτικών μέτρων και δράσεων επιβολής υπό το πρίσμα των αποτελεσμάτων των αξιολογήσεων από ομοτίμους που αναφέρονται στο άρθρο 16·

   γ) ένας δείκτης κυβερνοασφάλειας που παρέχει συγκεντρωτική αξιολόγηση του επιπέδου ωριμότητας των ικανοτήτων κυβερνοασφάλειας.

2. Η έκθεση περιλαμβάνει συγκεκριμένες συστάσεις πολιτικής για την αύξηση του επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση και σύνοψη των ευρημάτων 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.

Άρθρο 16

Αξιολογήσεις από ομότιμους

1. Κατόπιν διαβούλευσης με την ομάδα συνεργασίας και τον ENISA, και το αργότερο 18 μήνες μετά την έναρξη ισχύος της παρούσας οδηγίας, η Επιτροπή καθορίζει τη μεθοδολογία και το περιεχόμενο ενός συστήματος αξιολόγησης από ομοτίμους για την αξιολόγηση της αποτελεσματικότητας των πολιτικών κυβερνοασφάλειας των κρατών μελών. Οι αξιολογήσεις διενεργούνται από τεχνικούς εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας οι οποίοι προέρχονται από κράτη μέλη διαφορετικά από το κράτος που υποβάλλεται σε αξιολόγηση και καλύπτουν τουλάχιστον τα εξής:

   i) την αποτελεσματικότητα της εφαρμογής των απαιτήσεων διαχείρισης κινδύνων για την κυβερνοασφάλεια και των υποχρεώσεων αναφοράς περιστατικών που αναφέρονται στα άρθρα 18 και 20·

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

   iii) τις επιχειρησιακές ικανότητες και την αποτελεσματικότητα των CSIRT·

   iv) την αποτελεσματικότητα της αμοιβαίας συνδρομής που αναφέρεται στο άρθρο 34·

   v) την αποτελεσματικότητα του πλαισίου ανταλλαγής πληροφοριών που αναφέρεται στο άρθρο 26 της παρούσας οδηγίας.

2. Η μεθοδολογία περιλαμβάνει αντικειμενικά, δίκαια και διαφανή κριτήρια χωρίς διακρίσεις βάσει των οποίων τα κράτη μέλη ορίζουν εμπειρογνώμονες επιλέξιμους για τη διενέργεια των αξιολογήσεων από ομοτίμους. Ο ENISA και η Επιτροπή ορίζουν εμπειρογνώμονες οι οποίοι συμμετέχουν ως παρατηρητές στις αξιολογήσεις από ομοτίμους. Η Επιτροπή, με την υποστήριξη του ENISA, καθορίζει, στο πλαίσιο της μεθοδολογίας που αναφέρεται στην παράγραφο 1, αντικειμενικό, δίκαιο και διαφανές σύστημα χωρίς διακρίσεις για την επιλογή και τον τυχαίο διορισμό εμπειρογνωμόνων σε κάθε αξιολόγηση από ομοτίμους.

3. Οι οργανωτικές πτυχές των αξιολογήσεων από ομοτίμους αποφασίζονται από την Επιτροπή, με την υποστήριξη του ENISA, και, κατόπιν διαβούλευσης με την ομάδα συνεργασίας, βασίζονται σε κριτήρια που καθορίζονται στη μεθοδολογία που αναφέρεται στην παράγραφο 1. Στις αξιολογήσεις από ομοτίμους αξιολογούνται οι πτυχές που αναφέρονται στην παράγραφο 1 για όλα τα κράτη μέλη και όλους τους τομείς, συμπεριλαμβανομένων στοχευμένων ζητημάτων που αφορούν συγκεκριμένα ένα ή περισσότερα κράτη μέλη ή έναν ή περισσότερους τομείς.

4. Στο πλαίσιο των αξιολογήσεων από ομοτίμους πραγματοποιούνται πραγματικές ή εικονικές επιτόπιες επισκέψεις και ανταλλαγές εκτός των εγκαταστάσεων. Με γνώμονα την αρχή της καλής συνεργασίας, τα κράτη μέλη που υποβάλλονται σε αξιολόγηση παρέχουν στους ορισθέντες εμπειρογνώμονες τις πληροφορίες που τους ζητούνται και που είναι αναγκαίες για την αξιολόγηση των πτυχών της αξιολόγησης. Κάθε πληροφορία που λαμβάνεται μέσω της διαδικασίας αξιολόγησης από

ομοτίμους χρησιμοποιείται αποκλειστικά για τον σκοπό αυτό. Οι εμπειρογνώμονες που συμμετέχουν στην αξιολόγηση από ομοτίμους δεν αποκαλύπτουν σε τρίτους τυχόν ευαίσθητες ή εμπιστευτικές πληροφορίες που απέκτησαν κατά τη διάρκεια της εν λόγω αξιολόγησης.

5. Οι πτυχές που αξιολογούνται 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 την Επιτροπή, κατόπιν διαβούλευσης με τον ENISA και την ομάδα συνεργασίας.

6. Τα κράτη μέλη μεριμνούν για τη γνωστοποίηση οποιουδήποτε κινδύνου σύγκρουσης συμφερόντων που αφορά τους ορισθέντες εμπειρογνώμονες στα άλλα κράτη μέλη, στην Επιτροπή και στον ENISA χωρίς αδικαιολόγητη καθυστέρηση.

7. Οι εμπειρογνώμονες που συμμετέχουν σε αξιολογήσεις από ομοτίμους συντάσσουν εκθέσεις με τα ευρήματα και τα συμπεράσματα των αξιολογήσεων. Οι εκθέσεις υποβάλλονται στην Επιτροπή, στην ομάδα συνεργασίας, στο δίκτυο CSIRT και στον ENISA. Οι εκθέσεις συζητούνται στην ομάδα συνεργασίας και στο δίκτυο CSIRT. Οι εκθέσεις μπορεί να δημοσιεύονται στον ειδικό ιστότοπο της ομάδας συνεργασίας.

ΚΕΦΑΛΑΙΟ IV

Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και υποχρεώσεις αναφοράς περιστατικών

ΤΜΗΜΑ I

Διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και αναφορά περιστατικών

Άρθρο 17

Διακυβέρνηση

1. Τα κράτη μέλη διασφαλίζουν ότι τα διοικητικά όργανα βασικών και σημαντικών οντοτήτων εγκρίνουν τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνονται από τις εν λόγω οντότητες προκειμένου να συμμορφωθούν με το άρθρο 18, εποπτεύουν την εφαρμογή τους και λογοδοτούν για τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που απορρέουν από το παρόν άρθρο.

2. Τα κράτη μέλη διασφαλίζουν ότι τα μέλη του διοικητικού οργάνου παρακολουθούν, σε τακτική βάση, ειδικά προγράμματα κατάρτισης για την απόκτηση επαρκών γνώσεων και δεξιοτήτων ώστε να αντιλαμβάνονται και να αξιολογούν τους κινδύνους για την κυβερνοασφάλεια και τις πρακτικές διαχείρισής τους, καθώς και τον αντίκτυπό τους στις δραστηριότητες της οντότητας.

Άρθρο 18

Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας

1. Τα κράτη μέλη εξασφαλίζουν ότι οι βασικές και σημαντικές οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν οι εν λόγω οντότητες κατά την παροχή των υπηρεσιών τους. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων ανάλογο προς τον εκάστοτε κίνδυνο.

2. Στα μέτρα που αναφέρονται στην παράγραφο 1 περιλαμβάνονται τουλάχιστον τα ακόλουθα:

   α) πολιτικές ανάλυσης κινδύνων και ασφάλειας του πληροφοριακού συστήματος·

   β) χειρισμός περιστατικών (πρόληψη, ανίχνευση και αντιμετώπιση περιστατικών)·

   γ) συνέχιση των δραστηριοτήτων και διαχείριση των κρίσεων·

   δ) η ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ της κάθε οντότητας και των προμηθευτών της ή των παρόχων υπηρεσιών, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή υπηρεσιών διαχείρισης ασφάλειας·

   ε) η ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση δικτυακών και πληροφοριακών συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης τρωτών σημείων·

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

   ζ) η χρήση της κρυπτογράφησης και της κρυπτοθέτησης.

3. Τα κράτη μέλη διασφαλίζουν ότι, κατά την εξέταση των κατάλληλων μέτρων που αναφέρονται στην παράγραφο 2 στοιχείο δ), οι οντότητες λαμβάνουν υπόψη τα τρωτά σημεία που χαρακτηρίζουν κάθε προμηθευτή και πάροχο υπηρεσιών, καθώς και τη συνολική ποιότητα των προϊόντων και πρακτικών κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των ασφαλών διαδικασιών ανάπτυξής τους.

4. Τα κράτη μέλη διασφαλίζουν ότι, όταν μια οντότητα διαπιστώνει ότι οι υπηρεσίες ή τα καθήκοντά της, αντίστοιχα, δεν συνάδουν με τις απαιτήσεις της παραγράφου 2, λαμβάνει, χωρίς αδικαιολόγητη καθυστέρηση, όλα τα αναγκαία διορθωτικά μέτρα για να εξασφαλίσει τη συμμόρφωση της σχετικής υπηρεσίας.

5. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών προδιαγραφών των στοιχείων που αναφέρονται στην παράγραφο 2. Κατά την εκπόνηση των εν λόγω πράξεων, η Επιτροπή ενεργεί σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 37 παράγραφος 2 και ακολουθεί, στον μέγιστο δυνατό βαθμό, τα διεθνή και ευρωπαϊκά πρότυπα, καθώς και τις σχετικές τεχνικές προδιαγραφές.

6. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 36, για τη συμπλήρωση των στοιχείων που ορίζονται στην παράγραφο 2, ώστε να λαμβάνονται υπόψη νέες κυβερνοαπειλές, τεχνολογικές εξελίξεις ή τομεακές ιδιαιτερότητες.

Άρθρο 19

Συντονισμένες από την ΕΕ 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, συστημάτων ή προϊόντων αλυσίδων εφοδιασμού ΤΠΕ, λαμβάνοντας υπόψη τεχνικούς και, κατά περίπτωση, μη τεχνικούς παράγοντες κινδύνου.
2. Η Επιτροπή, κατόπιν διαβούλευσης με την ομάδα συνεργασίας και τον ENISA, προσδιορίζει τις συγκεκριμένες κρίσιμες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ που ενδέχεται να υπόκεινται στη συντονισμένη εκτίμηση κινδύνου που αναφέρεται στην παράγραφο 1.

Άρθρο 20

Υποχρεώσεις αναφοράς περιστατικών

1. Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις αρμόδιες αρχές ή στην CSIRT, σύμφωνα με τις παραγράφους 3 και 4, κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους. Κατά περίπτωση, οι εν λόγω οντότητες κοινοποιούν στους αποδέκτες των υπηρεσιών τους χωρίς αδικαιολόγητη καθυστέρηση περιστατικά που ενδέχεται να επηρεάσουν δυσμενώς την παροχή των εν λόγω υπηρεσιών. Τα κράτη μέλη διασφαλίζουν ότι οι εν λόγω οντότητες αναφέρουν, μεταξύ άλλων, κάθε πληροφορία που επιτρέπει στις αρμόδιες αρχές ή στην CSIRT να προσδιορίσουν τυχόν διασυνοριακές επιπτώσεις του περιστατικού.
2. Τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις αρμόδιες αρχές ή στην CSIRT κάθε σημαντική κυβερνοαπειλή την οποία εντοπίζουν οι εν λόγω οντότητες και η οποία θα μπορούσε ενδεχομένως να οδηγήσει σε σημαντικό περιστατικό.

   Κατά περίπτωση, οι εν λόγω οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στους αποδέκτες των υπηρεσιών τους που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή τυχόν μέτρα ή διορθωτικά μέτρα που μπορούν να λάβουν οι εν λόγω αποδέκτες για την αντιμετώπιση της εν λόγω απειλής. Κατά περίπτωση, οι οντότητες ενημερώνουν επίσης τους εν λόγω αποδέκτες για την ίδια την απειλή. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τη σχετική οντότητα.
3. Ένα περιστατικό θεωρείται σημαντικό σε περίπτωση που:

   α) προκάλεσε ή έχει τη δυνατότητα να προκαλέσει σημαντική λειτουργική διαταραχή ή οικονομικές ζημίες στην οικεία οντότητα·

β) έχει επηρεάσει ή έχει τη δυνατότητα να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντικές υλικές ή μη υλικές ζημίες.

4. Τα κράτη μέλη διασφαλίζουν ότι, για τους σκοπούς της κοινοποίησης δυνάμει της παραγράφου 1, οι οικείες οντότητες υποβάλλουν στις αρμόδιες αρχές ή στην CSIRT:

α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έλαβαν γνώση του συμβάντος, μια αρχική κοινοποίηση, στην οποία, κατά περίπτωση, αναφέρεται αν το περιστατικό προκλήθηκε πιθανώς από παράνομη ή κακόβουλη ενέργεια·

β) κατόπιν αιτήματος αρμόδιας αρχής ή CSIRT, ενδιάμεση έκθεση σχετικά με την εξέλιξη της κατάστασης·

γ) τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της έκθεσης βάσει του στοιχείου α), η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:

i) λεπτομερή περιγραφή του περιστατικού, 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.

Τα κράτη μέλη προβλέπουν ότι, σε δεόντως αιτιολογημένες περιπτώσεις και σε συμφωνία με τις αρμόδιες αρχές ή την CSIRT, η οικεία οντότητα μπορεί να παρεκκλίνει από τις προθεσμίες που ορίζονται στα στοιχεία α) και γ).

5. Οι αρμόδιες εθνικές αρχές ή η CSIRT παρέχουν, εντός 24 ωρών από την παραλαβή της αρχικής κοινοποίησης που αναφέρεται στην παράγραφο 4 στοιχείο α), απάντηση στη κοινοποιούσα οντότητα, συμπεριλαμβανομένης αρχικής ανατροφοδότησης σχετικά με το περιστατικό και, κατόπιν αιτήματος της οντότητας, καθοδήγηση σχετικά με την εφαρμογή πιθανών μέτρων μετριασμού. Σε περίπτωση που η CSIRT δεν έλαβε τη κοινοποίηση που αναφέρεται στην παράγραφο 1, η καθοδήγηση παρέχεται από την αρμόδια αρχή σε συνεργασία με την CSIRT. Η CSIRT παρέχει πρόσθετη τεχνική υποστήριξη κατόπιν αιτήματος της ενδιαφερόμενης οντότητας. Όταν υπάρχουν υπόνοιες ότι το περιστατικό είναι εγκληματικού χαρακτήρα, οι αρμόδιες εθνικές αρχές ή η CSIRT παρέχουν επίσης καθοδήγηση σχετικά με την αναφορά του περιστατικού στις αρχές επιβολής του νόμου.

6. Κατά περίπτωση, και ιδίως όταν το περιστατικό που αναφέρεται στην παράγραφο 1 αφορά δύο ή περισσότερα κράτη μέλη, η αρμόδια αρχή ή η CSIRT ενημερώνουν τα λοιπά επηρεαζόμενα κράτη μέλη και τον ENISA για το περιστατικό. Στο πλαίσιο της ενημέρωσης αυτής, οι αρμόδιες αρχές, οι CSIRT και τα ενιαία σημεία επαφής, σύμφωνα με το ενωσιακό δίκαιο, ή με την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα της οντότητας, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί.

7. Όταν η ευαισθητοποίηση του κοινού είναι απαραίτητη για την πρόληψη περιστατικού ή για την αντιμετώπιση εν εξελίξει περιστατικού, ή όταν η γνωστοποίηση του περιστατικού εξυπηρετεί άλλως το δημόσιο συμφέρον, η αρμόδια αρχή ή η CSIRT και, κατά περίπτωση, οι αρχές ή οι CSIRT άλλων ενδιαφερόμενων κρατών μελών μπορούν, κατόπιν διαβούλευσης με την ενδιαφερόμενη οντότητα, να ενημερώνουν το κοινό σχετικά με το συμβάν ή να απαιτούν από την οντότητα να το πράξει.

8. Κατόπιν αιτήματος της αρμόδιας αρχής ή της CSIRT, το ενιαίο σημείο επαφής διαβιβάζει τις κοινοποιήσεις που παραλήφθηκαν δυνάμει των παραγράφων 1 και 2 στα ενιαία κέντρα επαφής άλλων επηρεαζόμενων κρατών μελών.

9. Το ενιαίο σημείο επαφής υποβάλλει στον ENISA σε μηνιαία βάση συνοπτική έκθεση που περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με περιστατικά, σημαντικές κυβερνοαπειλές και παρ' ολίγον περιστατικά που κοινοποιούνται σύμφωνα με τις παραγράφους 1 και 2 και σύμφωνα με το άρθρο 27. Προκειμένου να συμβάλει στην παροχή συγκρίσιμων πληροφοριών, ο ENISA μπορεί να εκδώσει τεχνική καθοδήγηση σχετικά με τις παραμέτρους των πληροφοριών που περιλαμβάνονται στη συνοπτική έκθεση.

10. Οι αρμόδιες αρχές παρέχουν στις αρμόδιες αρχές που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων] πληροφορίες σχετικά με περιστατικά και κυβερνοαπειλές που κοινοποιούνται σύμφωνα με τις παραγράφους 1 και 2 από βασικές οντότητες που έχουν χαρακτηριστεί κρίσιμες οντότητες ή οντότητες ισοδύναμες με κρίσιμες οντότητες, σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων].

11. Η Επιτροπή μπορεί να εκδίδει εκτελεστικές πράξεις με τις οποίες προσδιορίζεται περαιτέρω το είδος των πληροφοριών, το μορφότυπο και η διαδικασία κοινοποίησης που υποβάλλεται σύμφωνα με τις παραγράφους 1 και 2. Η Επιτροπή μπορεί επίσης να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό, όπως αναφέρεται στην παράγραφο 3. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 37 παράγραφος 2.

Άρθρο 21

Χρήση των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας

1. Προκειμένου να αποδειχθεί η συμμόρφωση με ορισμένες απαιτήσεις του άρθρου 18, τα κράτη μέλη μπορούν να απαιτούν από βασικές και σημαντικές οντότητες να πιστοποιούν ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ στο πλαίσιο συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881. Τα προϊόντα, οι υπηρεσίες και οι διαδικασίες που υπόκεινται σε πιστοποίηση μπορούν να αναπτυχθούν από βασική ή σημαντική οντότητα ή να παρασχεθούν από τρίτους.

2. Η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις με τις οποίες θα προσδιορίζεται από ποιες κατηγορίες βασικών οντοτήτων θα απαιτείται η λήψη πιστοποιητικού και δυνάμει ποιων συγκεκριμένα ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας σύμφωνα με την παράγραφο 1. Οι κατ' εξουσιοδότηση πράξεις εκδίδονται σύμφωνα με το άρθρο 36.

3. Η Επιτροπή μπορεί να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα σύμφωνα με το άρθρο 48 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881 στις περιπτώσεις που δεν υπάρχει διαθέσιμο κατάλληλο ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας για τους σκοπούς της παραγράφου 2.

Άρθρο 22

Τυποποίηση

1. Για να προωθήσουν τη συγκλίνουσα εφαρμογή του άρθρου 18 παράγραφοι 1 και 2, τα κράτη μέλη, χωρίς να επιβάλλουν ούτε να ευνοούν τη χρησιμοποίηση συγκεκριμένου είδους τεχνολογίας, ενθαρρύνουν τη χρήση ευρωπαϊκών ή διεθνώς αποδεκτών προτύπων και προδιαγραφών σχετικών με την ασφάλεια δικτυακών και πληροφοριακών συστημάτων.

2. Ο ENISA, σε συνεργασία με τα κράτη μέλη, εκδίδει συμβουλές και κατευθυντήριες γραμμές όσον αφορά τους τεχνικούς τομείς που θα πρέπει να εξεταστούν σε σχέση με την παράγραφο 1, καθώς και όσον αφορά ήδη υφιστάμενα πρότυπα, συμπεριλαμβανομένων των εθνικών προτύπων των κρατών μελών, για την κάλυψη αυτών των τομέων.

Άρθρο 23

Βάσεις δεδομένων με ονόματα τομέα και δεδομένα καταχώρισης

1. Για τους σκοπούς της συμβολής στην ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του συστήματος ονομάτων τομέα (DNS), τα κράτη μέλη διασφαλίζουν ότι τα μητρώα τομέα ανωτάτου επιπέδου (TLD) και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για μητρώα TLD συλλέγουν και διατηρούν ακριβή και πλήρη δεδομένα καταχώρισης ονομάτων τομέα σε ειδική βάση δεδομένων με τη δέουσα επιμέλεια τηρώντας τη νομοθεσία της Ένωσης για την προστασία των δεδομένων όσον αφορά τα δεδομένα προσωπικού χαρακτήρα.

2. Τα κράτη μέλη διασφαλίζουν ότι οι βάσεις δεδομένων καταχώρισης ονομάτων τομέα που αναφέρονται στην παράγραφο 1 περιέχουν σχετικές πληροφορίες για τον εντοπισμό και την επικοινωνία με τους κατόχους των ονομάτων τομέα και τα σημεία επαφής που διαχειρίζονται τα ονόματα τομέα στο πλαίσιο των TLD.

3. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD διαθέτουν πολιτικές και διαδικασίες που διασφαλίζουν ότι οι βάσεις δεδομένων περιλαμβάνουν ακριβείς και πλήρεις πληροφορίες. Τα κράτη μέλη διασφαλίζουν ότι οι εν λόγω πολιτικές και διαδικασίες δημοσιοποιούνται.

4. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD δημοσιεύουν, χωρίς αδικαιολόγητη καθυστέρηση μετά την καταχώριση ονόματος τομέα, τα δεδομένα καταχώρισης τομέα που δεν αποτελούν δεδομένα προσωπικού χαρακτήρα.

5. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD παρέχουν πρόσβαση σε συγκεκριμένα δεδομένα καταχώρισης ονομάτων τομέα κατόπιν νόμιμων και δεόντως αιτιολογημένων αιτημάτων νόμιμων αιτούντων πρόσβαση, σύμφωνα με τη νομοθεσία της Ένωσης για την προστασία των δεδομένων. Τα κράτη μέλη διασφαλίζουν ότι τα μητρώα TLD και οι οντότητες που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα για τον TLD ανταποκρίνονται χωρίς αδικαιολόγητη καθυστέρηση σε όλα τα αιτήματα πρόσβασης. Τα κράτη μέλη διασφαλίζουν ότι οι πολιτικές και οι διαδικασίες γνωστοποίησης των εν λόγω δεδομένων δημοσιοποιούνται.

Τμήμα ΙΙ

Δικαιοδοσία και καταχώριση

Άρθρο 24

Δικαιοδοσία και εδαφικότητα

1. Οι πάροχοι υπηρεσιών DNS, τα μητρώα ονομάτων TLD, οι πάροχοι υπηρεσιών νεφοϋπολογιστικής, οι πάροχοι υπηρεσιών κέντρου δεδομένων και οι πάροχοι δικτύων διανομής περιεχομένου που αναφέρονται στο παράρτημα Ι σημείο 8, καθώς και οι πάροχοι ψηφιακών υπηρεσιών που αναφέρονται στο παράρτημα ΙΙ σημείο 6 θεωρείται ότι υπάγονται στη δικαιοδοσία του κράτους μέλους στο οποίο έχουν την κύρια εγκατάστασή τους στην Ένωση.

2. Για τους σκοπούς της παρούσας οδηγίας, οι οντότητες που αναφέρονται στην παράγραφο 1 θεωρείται ότι έχουν την κύρια εγκατάστασή τους στην Ένωση στο κράτος μέλος όπου λαμβάνονται οι αποφάσεις σχετικά με τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας. Εάν οι αποφάσεις αυτές δεν λαμβάνονται σε κάποια εγκατάσταση στην Ένωση, η κύρια εγκατάσταση θεωρείται ότι βρίσκεται στο κράτος μέλος στο οποίο οι οντότητες έχουν την εγκατάσταση με τον μεγαλύτερο αριθμό εργαζομένων στην Ένωση.

3. Εάν μια οντότητα που αναφέρεται στην παράγραφο 1 δεν είναι εγκατεστημένη στην Ένωση, αλλά παρέχει 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. Εάν δεν έχει οριστεί εκπρόσωπος εντός της Ένωσης δυνάμει του παρόντος άρθρου, κάθε κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες μπορεί να κινήσει νομικές διαδικασίες κατά της οντότητας για μη συμμόρφωση με τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία.

4. Ο ορισμός εκπροσώπου από οντότητα που αναφέρεται στην παράγραφο 1 δεν θίγει τις νομικές ενέργειες οι οποίες μπορούν να αναληφθούν κατά της ίδιας της οντότητας.

Άρθρο 25

Μητρώο βασικών και σημαντικών οντοτήτων

1. Ο ENISA δημιουργεί και διατηρεί μητρώο με τις βασικές και τις σημαντικές οντότητες που αναφέρονται στο άρθρο 24 παράγραφος 1. Οι οντότητες υποβάλλουν τις ακόλουθες πληροφορίες στον ENISA [το αργότερο έως 12 μήνες από την έναρξη ισχύος της οδηγίας]:

   α) την επωνυμία της οντότητας·

   β) τη διεύθυνση της κύριας εγκατάστασής της και των άλλων νόμιμων εγκαταστάσεών της στην Ένωση ή, εάν δεν είναι εγκατεστημένη στην Ένωση, του εκπροσώπου της που έχει οριστεί σύμφωνα με το άρθρο 24 παράγραφος 3·

γ) επικαιροποιημένα στοιχεία επικοινωνίας, συμπεριλαμβανομένων των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των αριθμών τηλεφώνου των οντοτήτων.

2. Οι οντότητες που αναφέρονται στην παράγραφο 1 κοινοποιούν στον ENISA τυχόν αλλαγές στα στοιχεία που υπέβαλαν σύμφωνα με την παράγραφο 1 χωρίς καθυστέρηση και, σε κάθε περίπτωση, εντός τριών μηνών από την ημερομηνία πραγματοποίησης της αλλαγής.

3. Μόλις λάβει τις πληροφορίες βάσει της παραγράφου 1, ο ENISA τις διαβιβάζει στα ενιαία σημεία επαφής, ανάλογα με την αναφερόμενη τοποθεσία της κύριας εγκατάστασης κάθε οντότητας ή, εάν αυτή δεν είναι εγκατεστημένη στην Ένωση, του εκπροσώπου που έχει ορίσει. Όταν μια οντότητα που αναφέρεται στην παράγραφο 1 διαθέτει πέραν της κύριας εγκατάστασής της στην Ένωση περαιτέρω εγκαταστάσεις σε άλλα κράτη μέλη, ο ENISA ενημερώνει επίσης τα ενιαία σημεία επαφής των εν λόγω κρατών μελών.

4. Σε περίπτωση που μια οντότητα δεν έχει καταχωρίσει τη δραστηριότητά της ή δεν παράσχει τις σχετικές πληροφορίες εντός της προθεσμίας που ορίζεται στην παράγραφο 1, έκαστο κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες είναι αρμόδιο να διασφαλίσει τη συμμόρφωση της εν λόγω οντότητας με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία.

ΚΕΦΑΛΑΙΟ V

Ανταλλαγή πληροφοριών

Άρθρο 26

Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας

1. Με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679, τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες μπορούν να ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες για την κυβερνοασφάλεια, μεταξύ άλλων πληροφορίες για κυβερνοαπειλές, τρωτά σημεία, δείκτες έκθεσης σε κίνδυνο, τακτικές, τεχνικές και διαδικασίες, προειδοποιήσεις για την κυβερνοασφάλεια και εργαλεία παραμετροποίησης, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

   α) αποσκοπεί στην πρόληψη, τον εντοπισμό, την αντιμετώπιση ή τον μετριασμό περιστατικών·

   β) ενισχύει το επίπεδο κυβερνοασφάλειας, ιδίως μέσω της ευαισθητοποίησης σε σχέση με τις κυβερνοαπειλές, του περιορισμού ή της παρεμπόδισης της ικανότητας διάδοσης των εν λόγω απειλών, της στήριξης μιας σειράς αμυντικών ικανοτήτων, της αποκατάστασης και γνωστοποίησης τρωτών σημείων, των τεχνικών ανίχνευσης απειλών, των στρατηγικών μετριασμού ή των σταδίων αντίδρασης και ανάκαμψης.

2. Τα κράτη μέλη διασφαλίζουν ότι η ανταλλαγή πληροφοριών πραγματοποιείται στο πλαίσιο αξιόπιστων κοινοτήτων βασικών και σημαντικών οντοτήτων. Η ανταλλαγή αυτή πραγματοποιείται βάσει ρυθμίσεων ανταλλαγής πληροφοριών όσον αφορά τον

δυνητικά ευαίσθητο χαρακτήρα των ανταλλασσόμενων πληροφοριών και σύμφωνα με τους κανόνες του δικαίου της Ένωσης που αναφέρονται στην παράγραφο 1.

3. Τα κράτη μέλη θεσπίζουν κανόνες που προσδιορίζουν τη διαδικασία, τα επιχειρησιακά στοιχεία (συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠΕ), το περιεχόμενο και τους όρους των ρυθμίσεων ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 2. Οι εν λόγω κανόνες καθορίζουν επίσης τις λεπτομέρειες της συμμετοχής των δημόσιων αρχών στις εν λόγω ρυθμίσεις, καθώς και τα επιχειρησιακά στοιχεία, συμπεριλαμβανομένης της χρήσης ειδικών πλατφορμών ΤΠ. Τα κράτη μέλη παρέχουν στήριξη για την εφαρμογή των εν λόγω ρυθμίσεων σύμφωνα με τις πολιτικές τους που αναφέρονται στο άρθρο 5 παράγραφος 2 στοιχείο ζ).

4. Οι βασικές και σημαντικές οντότητες γνωστοποιούν στις αρμόδιες αρχές τη συμμετοχή τους στις ρυθμίσεις ανταλλαγής πληροφοριών που αναφέρονται στην παράγραφο 2, μόλις προσχωρήσουν στις εν λόγω ρυθμίσεις ή, ανάλογα με την περίπτωση, την ανάκληση της συμμετοχής τους στις ρυθμίσεις αυτές, μόλις τεθεί σε ισχύ η απόσυρση.

5. Σύμφωνα με το ενωσιακό δίκαιο, ο ENISA στηρίζει τη θέσπιση ρυθμίσεων για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας που αναφέρονται στην παράγραφο 2, παρέχοντας βέλτιστες πρακτικές και καθοδήγηση.

Άρθρο 27

Εθελούσια κοινοποίηση των σχετικών πληροφοριών

Τα κράτη μέλη διασφαλίζουν ότι, με την επιφύλαξη του άρθρου 3, οι οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας μπορούν να υποβάλλουν κοινοποιήσεις, σε εθελοντική βάση, για σημαντικά συμβάντα, κυβερνοαπειλές ή παρ' ολίγον περιστατικά. Κατά την επεξεργασία των κοινοποιήσεων, τα κράτη μέλη ενεργούν σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 20. Τα κράτη μέλη μπορούν να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων. Η εθελούσια αναφορά δεν συνεπάγεται την επιβολή στην αναφέρουσα οντότητα πρόσθετων υποχρεώσεων τις οποίες δεν θα υπείχε αν δεν προέβαινε στην κοινοποίηση.

ΚΕΦΑΛΑΙΟ VI

Εποπτεία και επιβολή

Άρθρο 28

Γενικές πτυχές που αφορούν την εποπτεία και την επιβολή

1. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές παρακολουθούν αποτελεσματικά και λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν τη συμμόρφωση με την παρούσα οδηγία, ιδίως με τις υποχρεώσεις που ορίζονται στα άρθρα 18 και 20.

2. Κατά την αντιμετώπιση περιστατικών που οδηγούν σε παραβιάσεις προσωπικών δεδομένων, οι αρμόδιες αρχές συνεργάζονται στενά με τις αρχές προστασίας δεδομένων.

Άρθρο 29

Εποπτεία και επιβολή όσον αφορά τις 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:

   α) επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένων δειγματοληπτικών ελέγχων·

   β) τακτικούς ελέγχους·

   γ) στοχευμένους ελέγχους ασφάλειας με βάση εκτιμήσεις κινδύνου ή διαθέσιμες πληροφορίες σχετικά με τον κίνδυνο·

   δ) σαρώσεις ασφάλειας που βασίζονται σε αντικειμενικά, αμερόληπτα, δίκαια και διαφανή κριτήρια αξιολόγησης κινδύνου·

   ε) αιτήματα παροχής πληροφοριών που είναι αναγκαίες για την αξιολόγηση των μέτρων κυβερνοασφάλειας που λαμβάνει η οντότητα, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και συμμόρφωση με την υποχρέωση κοινοποίησης στον ENISA σύμφωνα με το άρθρο 25 παράγραφοι 1 και 2·

   στ) αιτήματα πρόσβασης σε δεδομένα, έγγραφα ή 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.

3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχεία ε) έως ζ), 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 εξουσιών τους επιβολής σε σχέση με βασικές οντότητες, δύνανται:

   α) να εκδίδουν προειδοποιήσεις σχετικά με τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία·

   β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις εν λόγω οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή τις παραβάσεις των υποχρεώσεων που ορίζονται στην παρούσα οδηγία·

   γ) να διατάσσουν τις εν λόγω οντότητες να παύσουν συμπεριφορά που δεν συμμορφώνεται προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·

δ) να διατάσσουν τις εν λόγω οντότητες να προβούν σε συμμόρφωση των μέτρων διαχείρισης κινδύνου και/ή των υποχρεώσεων αναφοράς περιστατικών προς τις υποχρεώσεις που ορίζονται στα άρθρα 18 και 20 με συγκεκριμένο τρόπο και εντός καθορισμένης προθεσμίας·

ε) να διατάσσουν τις εν λόγω οντότητες να ενημερώνουν το φυσικό ή νομικό πρόσωπο (ή πρόσωπα), στα οποία παρέχουν υπηρεσίες ή δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, για τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να ληφθούν από το εν λόγω φυσικό ή νομικό πρόσωπο (ή πρόσωπα) για την αντιμετώπιση της εν λόγω απειλής·

στ) να διατάσσουν τις εν λόγω οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν κατόπιν ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να ορίζουν υπεύθυνο παρακολούθησης με σαφώς προσδιορισμένα καθήκοντα για καθορισμένο χρονικό διάστημα, προκειμένου να επιβλέπει τη συμμόρφωση με τις υποχρεώσεις τους που προβλέπονται στα άρθρα 18 και 20·

η) να διατάσσουν τις εν λόγω οντότητες να δημοσιοποιούν πτυχές της μη συμμόρφωσης με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία με συγκεκριμένο τρόπο·

θ) να προβαίνουν σε δημόσια δήλωση στην οποία να προσδιορίζεται το νομικό και το φυσικό πρόσωπο (ή πρόσωπα) που ευθύνονται για την παράβαση υποχρέωσης που προβλέπεται στην παρούσα οδηγία και η φύση της εν λόγω παράβασης·

ι) να επιβάλλουν ή να ζητούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με την εθνική νομοθεσία, διοικητικού προστίμου δυνάμει του άρθρου 31 επιπροσθέτως ή αντί των μέτρων που αναφέρονται στα στοιχεία α) έως θ) της παρούσας παραγράφου, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

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

α) να αναστείλουν ή να ζητήσουν από φορέα πιστοποίησης ή εξουσιοδότησης να αναστείλει πιστοποίηση ή εξουσιοδότηση που αφορά μέρος ή το σύνολο των υπηρεσιών ή δραστηριοτήτων που παρέχονται από βασική οντότητα·

β) να επιβάλουν ή να ζητήσουν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, προσωρινή απαγόρευση κατά οποιουδήποτε προσώπου ασκεί διευθυντικά καθήκοντα σε επίπεδο γενικού διευθυντή ή νομικού εκπροσώπου στην εν λόγω βασική οντότητα, καθώς και οποιουδήποτε άλλου φυσικού προσώπου θεωρείται υπαίτιο για την παράβαση, να ασκούν διευθυντικά καθήκοντα στην εν λόγω οντότητα.

Οι κυρώσεις αυτές επιβάλλονται μόνο έως ότου η οντότητα λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή τη συμμόρφωση με τις απαιτήσεις της αρμόδιας αρχής για τις οποίες επιβλήθηκαν οι εν λόγω κυρώσεις.

6. Τα κράτη μέλη διασφαλίζουν ότι κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως αντιπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει τις εξουσίες να διασφαλίζει τη συμμόρφωσή της με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των καθηκόντων τους όσον αφορά την τήρηση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία.

7. Κατά τη λήψη μέτρων επιβολής ή την επιβολή κυρώσεων σύμφωνα με τις παραγράφους 4 και 5, οι αρμόδιες αρχές συμμορφώνονται με τα δικαιώματα της υπεράσπισης και λαμβάνουν υπόψη τις περιστάσεις κάθε μεμονωμένης περίπτωσης και, κατ' ελάχιστον, λαμβάνουν δεόντως υπόψη:

α) τη σοβαρότητα της παράβασης και τη σημασία των διατάξεων που παραβιάστηκαν. Στις παραβάσεις που θα πρέπει να θεωρούνται σοβαρές συγκαταλέγονται: επανειλημμένες παραβιάσεις, παράλειψη κοινοποίησης ή αποκατάστασης περιστατικών με αποτέλεσμα τη σημαντική διατάραξη, αδυναμία αποκατάστασης ελλείψεων σύμφωνα με δεσμευτικές οδηγίες των αρμόδιων αρχών, παρεμπόδιση των ελέγχων ή των δραστηριοτήτων παρακολούθησης που διατάσσονται από την αρμόδια αρχή μετά τη διαπίστωση παράβασης, παροχή ψευδών ή χονδροειδώς διαστρεβλωμένων πληροφοριών σε σχέση με τις απαιτήσεις διαχείρισης κινδύνου ή τις υποχρεώσεις αναφοράς περιστατικών που ορίζονται στα άρθρα 18 και 20.

β) η διάρκεια της παράβασης, συμπεριλαμβανομένου του στοιχείου των επανειλημμένων παραβάσεων·

γ) η πραγματική ζημία που προκλήθηκε ή οι απώλειες που προέκυψαν ή οι δυνητικές ζημίες ή απώλειες που θα μπορούσαν να έχουν προκληθεί, στον βαθμό που μπορούν να προσδιοριστούν. Κατά την αξιολόγηση αυτής της πτυχής, λαμβάνονται υπόψη, μεταξύ άλλων, οι πραγματικές ή δυνητικές χρηματοοικονομικές ή οικονομικές απώλειες, οι επιπτώσεις σε άλλες υπηρεσίες, ο αριθμός των χρηστών που επηρεάζονται ή ενδέχεται να επηρεαστούν·

δ) το αν η παράβαση διαπράχθηκε εκ προθέσεως ή εξ αμελείας·

ε) μέτρα που λαμβάνει η οντότητα για την πρόληψη ή τον μετριασμό της ζημίας ή/και των απωλειών·

στ) η τήρηση εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης·

ζ) ο βαθμός συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου (ή προσώπων) με τις αρμόδιες αρχές.

8. Οι αρμόδιες αρχές αιτιολογούν λεπτομερώς τις αποφάσεις τους όσον αφορά την επιβολή. Πριν από τη λήψη των εν λόγω αποφάσεων, οι αρμόδιες αρχές κοινοποιούν στις ενδιαφερόμενες οντότητες τα προκαταρκτικά πορίσματά τους και παρέχουν εύλογο χρονικό διάστημα στις εν λόγω οντότητες για να υποβάλουν τις παρατηρήσεις τους.

9. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές τους ενημερώνουν τις σχετικές αρμόδιες αρχές του οικείου κράτους μέλους που έχουν οριστεί σύμφωνα με την οδηγία (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων] κατά την άσκηση των εξουσιών τους εποπτείας και επιβολής με σκοπό

τη διασφάλιση της συμμόρφωσης βασικής οντότητας που έχει χαρακτηριστεί κρίσιμη ή ισοδύναμη με κρίσιμη οντότητα, δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων], προς τις υποχρεώσεις που απορρέουν από την παρούσα οδηγία. Κατόπιν αιτήματος των αρμόδιων αρχών δυνάμει της οδηγίας (ΕΕ) XXXX/XXXX [οδηγία σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων], οι αρμόδιες αρχές μπορούν να ασκούν τις εξουσίες τους εποπτείας και επιβολής σε βασική οντότητα που έχει χαρακτηριστεί κρίσιμη ή σε ισοδύναμη οντότητα.

Άρθρο 30

Εποπτεία και επιβολή όσον αφορά σημαντικές οντότητες

1. Όταν τους υποβάλλονται αποδεικτικά στοιχεία ή ενδείξεις ότι μια σημαντική οντότητα δεν συμμορφώνεται με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία, και ιδίως στα άρθρα 18 και 20, τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές αναλαμβάνουν δράση, όπου απαιτείται, μέσω εκ των υστέρων εποπτικών μέτρων.

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

   α) επιτόπιες επιθεωρήσεις και εκ των υστέρων εποπτεία εκτός των εγκαταστάσεων·

   β) στοχευμένους ελέγχους ασφάλειας με βάση εκτιμήσεις κινδύνου ή διαθέσιμες πληροφορίες σχετικά με τον κίνδυνο·

   γ) σαρώσεις ασφάλειας που βασίζονται σε αντικειμενικά, δίκαια και διαφανή κριτήρια αξιολόγησης κινδύνου·

   δ) αιτήματα για τυχόν πληροφορίες που είναι αναγκαίες για την εκ των υστέρων αξιολόγηση των μέτρων κυβερνοασφάλειας, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών κυβερνοασφάλειας, καθώς και συμμόρφωση με την υποχρέωση κοινοποίησης στον ENISA σύμφωνα με το άρθρο 25 παράγραφοι 1 και 2·

   ε) αιτήματα πρόσβασης σε δεδομένα, έγγραφα ή/και πληροφορίες που απαιτούνται για την εκτέλεση των εποπτικών καθηκόντων.

3. Κατά την άσκηση των εξουσιών τους δυνάμει της παραγράφου 2 στοιχεία δ) ή ε), 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 εξουσιών τους επιβολής σε σχέση με σημαντικές οντότητες, δύνανται:

   α) να εκδίδουν προειδοποιήσεις σχετικά με τη μη συμμόρφωση των οντοτήτων με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία·

   β) να εκδίδουν δεσμευτικές οδηγίες ή διαταγή προς τις εν λόγω οντότητες να αποκαταστήσουν τις διαπιστωθείσες ελλείψεις ή την παράβαση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία·

γ) να διατάσσουν τις εν λόγω οντότητες να παύσουν τη συμπεριφορά που δεν συμμορφώνεται προς τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία και να απόσχουν από την επανάληψη της εν λόγω συμπεριφοράς·

δ) να διατάσσουν τις εν λόγω οντότητες να προβούν σε συμμόρφωση των μέτρων διαχείρισης κινδύνου ή των υποχρεώσεων αναφοράς περιστατικών προς τις υποχρεώσεις που ορίζονται στα άρθρα 18 και 20 με συγκεκριμένο τρόπο και εντός καθορισμένης προθεσμίας·

ε) να διατάσσουν τις εν λόγω οντότητες να ενημερώνουν το φυσικό ή νομικό πρόσωπο (ή πρόσωπα), στα οποία παρέχουν υπηρεσίες ή δραστηριότητες που ενδέχεται να επηρεαστούν από σημαντική κυβερνοαπειλή, για τυχόν μέτρα προστασίας ή αποκατάστασης που μπορούν να ληφθούν από το εν λόγω φυσικό ή νομικό πρόσωπο (ή πρόσωπα) για την αντιμετώπιση της εν λόγω απειλής·

στ) να διατάσσουν τις εν λόγω οντότητες να εφαρμόσουν τις συστάσεις που διατυπώθηκαν κατόπιν ελέγχου ασφάλειας εντός εύλογης προθεσμίας·

ζ) να διατάσσουν τις εν λόγω οντότητες να δημοσιοποιούν πτυχές της μη συμμόρφωσης με τις υποχρεώσεις τους που ορίζονται στην παρούσα οδηγία με συγκεκριμένο τρόπο·

η) να προβαίνουν σε δημόσια δήλωση στην οποία να προσδιορίζεται το νομικό και το φυσικό πρόσωπο (ή πρόσωπα) που ευθύνονται για την παράβαση υποχρέωσης που προβλέπεται στην παρούσα οδηγία και η φύση της εν λόγω παράβασης·

θ) να επιβάλλουν ή να ζητούν την επιβολή από τα αρμόδια όργανα ή δικαστήρια, σύμφωνα με την εθνική νομοθεσία, διοικητικού προστίμου δυνάμει του άρθρου 31 επιπλέον ή αντί των μέτρων που αναφέρονται στα στοιχεία α) έως η) της παρούσας παραγράφου, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης.

5. Το άρθρο 29 παράγραφοι 6 έως 8 εφαρμόζεται επίσης στα μέτρα εποπτείας και επιβολής που προβλέπονται στο παρόν άρθρο για τις σημαντικές οντότητες που απαριθμούνται στο παράρτημα ΙΙ.

Άρθρο 31

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

1. Τα κράτη μέλη διασφαλίζουν ότι η επιβολή διοικητικών προστίμων σε βασικές και σε σημαντικές οντότητες σύμφωνα με το παρόν άρθρο για παραβάσεις των υποχρεώσεων που ορίζονται στην παρούσα οδηγία είναι, σε κάθε μεμονωμένη περίπτωση, αποτελεσματική, αναλογική και αποτρεπτική.

2. Τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο άρθρο 30 παράγραφος 4 στοιχεία α) έως η).

3. Όταν αποφασίζεται η ενδεχόμενη επιβολή διοικητικού προστίμου και το ύψος του σε κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη, κατ' ελάχιστον, τα στοιχεία που προβλέπονται στο άρθρο 29 παράγραφος 7.

4. Τα κράτη μέλη διασφαλίζουν ότι οι παραβάσεις των υποχρεώσεων που προβλέπονται στο άρθρο 18 ή στο άρθρο 20 υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα κατ' ανώτατο όριο ύψους τουλάχιστον 10 000 000 EUR ή έως 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η βασική ή σημαντική οντότητα κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο.

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

6. Με την επιφύλαξη των εξουσιών των αρμόδιων αρχών σύμφωνα με τα άρθρα 29 και 30, κάθε κράτος μέλος δύναται να καθορίζει τους κανόνες σχετικά με το εάν και σε ποιο βαθμό μπορούν να επιβάλλονται διοικητικά πρόστιμα σε φορείς της δημόσιας διοίκησης που αναφέρονται στο άρθρο 4 παράγραφος 23, με την επιφύλαξη των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία.

Άρθρο 32

Παραβάσεις που συνεπάγονται παραβίαση δεδομένων προσωπικού χαρακτήρα

1. Εάν οι αρμόδιες αρχές έχουν ενδείξεις ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 18 και 20 συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 2016/679, η οποία κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν τις εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του εν λόγω κανονισμού εντός εύλογου χρονικού διαστήματος.

2. Εάν οι εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του κανονισμού (ΕΕ) 2016/679 αποφασίσουν να ασκήσουν τις εξουσίες τους σύμφωνα με το άρθρο 58 στοιχείο θ) του εν λόγω κανονισμού και να επιβάλουν διοικητικό πρόστιμο, οι αρμόδιες αρχές δεν επιβάλλουν διοικητικό πρόστιμο για την ίδια παράβαση δυνάμει του άρθρου 31 της παρούσας οδηγίας. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόζουν τα μέτρα επιβολής ή να ασκούν τις εξουσίες επιβολής κυρώσεων που προβλέπονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο άρθρο 30 παράγραφος 4 στοιχεία α) έως η) 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 μπορεί να ενημερώσει την εποπτική αρχή που είναι εγκατεστημένη στο ίδιο κράτος μέλος.

Άρθρο 33

Κυρώσεις

1. Τα κράτη μέλη καθορίζουν τους κανόνες για τις κυρώσεις οι οποίες πρέπει να επιβάλλονται σε περίπτωση παράβασης των εθνικών διατάξεων που θεσπίζονται κατ' εφαρμογή της παρούσας οδηγίας και λαμβάνουν όλα τα αναγκαία μέτρα για να εξασφαλίσουν την επιβολή τους. Οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές.

2. Τα κράτη μέλη κοινοποιούν στην Επιτροπή, έως [δύο] έτη μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας, τους κανόνες και τα μέτρα αυτά και την ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση, για κάθε μεταγενέστερη τροποποίησή τους.

Άρθρο 34

Αμοιβαία συνδρομή

1. Εάν μια βασική ή σημαντική οντότητα παρέχει υπηρεσίες σε περισσότερα από ένα κράτη μέλη ή έχει την κύρια εγκατάστασή της ή εκπρόσωπο σε ένα κράτος μέλος αλλά τα δικτυακά και πληροφοριακά συστήματά της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, η αρμόδια αρχή του κράτους μέλους της κύριας ή άλλης εγκατάστασης ή του εκπροσώπου και οι αρμόδιες αρχές των άλλων κρατών μελών συνεργάζονται και παρέχουν αμοιβαία συνδρομή, εφόσον απαιτείται. 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 και τη συνέχεια που δίνεται σε αυτά, σύμφωνα με τα άρθρα 29 και 30·

   β) μια αρμόδια αρχή μπορεί να ζητήσει από άλλη αρμόδια αρχή να λάβει τα μέτρα εποπτείας ή επιβολής που αναφέρονται στα άρθρα 29 και 30·

   γ) μια αρμόδια αρχή, μόλις λάβει αιτιολογημένο αίτημα από άλλη αρμόδια αρχή, παρέχει συνδρομή στην άλλη αρμόδια αρχή, ώστε τα μέτρα εποπτείας ή επιβολής που αναφέρονται στα άρθρα 29 και 30 να μπορούν να εφαρμοστούν με αποτελεσματικό, αποδοτικό και συνεπή τρόπο. Η εν λόγω αμοιβαία συνδρομή μπορεί να καλύπτει αιτήματα παροχής πληροφοριών και μέτρα εποπτείας, συμπεριλαμβανομένων αιτημάτων για τη διενέργεια επιτόπιων επιθεωρήσεων ή εποπτείας εκτός των εγκαταστάσεων ή στοχευμένων ελέγχων ασφάλειας. Η αρμόδια αρχή στην οποία απευθύνεται αίτημα συνδρομής δεν μπορεί να αρνηθεί το εν λόγω αίτημα, εκτός εάν, κατόπιν ανταλλαγής απόψεων με τις άλλες ενδιαφερόμενες αρχές, τον ENISA και την Επιτροπή, διαπιστωθεί ότι είτε η αρχή δεν είναι αρμόδια να παράσχει την αιτούμενη συνδρομή είτε η αιτούμενη συνδρομή δεν είναι ανάλογη προς τα εποπτικά καθήκοντα της αρμόδιας αρχής που εκτελούνται σύμφωνα με το άρθρο 29 ή το άρθρο 30.

2. Κατά περίπτωση και με κοινή συμφωνία, αρμόδιες αρχές από διαφορετικά κράτη μέλη μπορούν να εκτελούν τις κοινές δράσεις εποπτείας που αναφέρονται στα άρθρα 29 και 30.

ΚΕΦΑΛΑΙΟ VII

Μεταβατικές και τελικές διατάξεις

Άρθρο 35

Επανεξέταση

Η Επιτροπή προβαίνει σε περιοδική επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Η έκθεση αξιολογεί ιδίως τη σημασία των τομέων, των υποτομέων, του μεγέθους και του είδους των οντοτήτων που αναφέρονται στα παραρτήματα Ι και ΙΙ 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 πρώτη έκθεση υποβάλλεται το αργότερο …[54 μήνες μετά την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας].

Άρθρο 36

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 18 παράγραφος 6 και στο άρθρο 21 παράγραφος 2 εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή για περίοδο πέντε ετών από [...]
3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 18 παράγραφος 6 και στο άρθρο 21 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 εκδώσει κατ' εξουσιοδότηση πράξη, 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. Αμέσως μετά την έκδοση κατ' εξουσιοδότηση πράξης, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.
6. Κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 18 παράγραφος 6 και του άρθρου 21 παράγραφος 2 τίθεται σε ισχύ μόνον εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο εντός δύο μηνών από την ημέρα που η πράξη κοινοποιείται στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν

αντιρρήσεις. Η περίοδος αυτή παρατείνεται κατά δύο μήνες με πρωτοβουλία του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Άρθρο 37

Διαδικασία επιτροπής

1. Η Επιτροπή επικουρείται από επιτροπή. Πρόκειται για επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.
2. Όταν γίνεται αναφορά 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.

Άρθρο 38

Μεταφορά στο εθνικό δίκαιο

1. Τα κράτη μέλη θεσπίζουν και δημοσιεύουν, έως … [18 μήνες από την ημερομηνία έναρξης ισχύος της παρούσας οδηγίας], τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν προς την παρούσα οδηγία. Ενημερώνουν αμέσως την Επιτροπή σχετικά. Θέτουν τα μέτρα αυτά σε εφαρμογή από … [μία ημέρα μετά την ημερομηνία που αναφέρεται στο πρώτο εδάφιο].
2. Οι διατάξεις αυτές, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν αναφορά στην παρούσα οδηγία ή συνοδεύονται από την αναφορά αυτή κατά την επίσημη δημοσίευσή τους. Ο τρόπος της αναφοράς αποφασίζεται από τα κράτη μέλη.

Άρθρο 39

Τροποποίηση του κανονισμού (ΕΚ) αριθ. 910/2014

Το άρθρο 19 του κανονισμού (ΕΕ) αριθ. 910/2014 απαλείφεται.

Άρθρο 40

Τροποποίηση της οδηγίας (ΕΕ) 2018/1972

Τα άρθρα 40 και 41 της οδηγίας 2018/1972/ΕΕ απαλείφονται.

Άρθρο 41

Κατάργηση

Η οδηγία (ΕΕ) 2016/1148 καταργείται από τις.. [ημερομηνία λήξης της προθεσμίας μεταφοράς της οδηγίας στο εθνικό δίκαιο].

Οι αναφορές στην οδηγία (ΕΕ) 2016/1148 θεωρούνται ως αναφορές στην παρούσα οδηγία και νοούνται σύμφωνα με τον πίνακα αντιστοιχίας του παραρτήματος ΙΙΙ.

Άρθρο 42

Θέση σε ισχύ

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

Άρθρο 43

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες,

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

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

Περιεχόμενα

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ 4

1.1. Τίτλος της πρότασης/πρωτοβουλίας 4

1.2. Σχετικοί τομείς πολιτικής *(ομάδα προγραμμάτων)* 4

1.3. Η πρόταση/πρωτοβουλία αφορά: 4

1.4. Αιτιολόγηση της πρότασης/πρωτοβουλίας 4

1.4.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας 4

1.4.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα. 4

1.4.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος 5

1.4.4. Συμβατότητα και ενδεχόμενη συνέργεια με άλλα κατάλληλα μέσα 5

1.5. Διάρκεια και δημοσιονομικές επιπτώσεις 6

1.6. Προβλεπόμενοι τρόποι διαχείρισης 6

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ 8

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων 8

2.2. Συστήματα διαχείρισης και ελέγχου 8

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου 8

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους 8

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο) 8

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας 8

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ 9

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και νέες γραμμές δαπανών του προϋπολογισμού που προτείνονται 9

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες 10

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες 10

3.2.2. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις πιστώσεις διοικητικού χαρακτήρα 13

3.2.3. Συμμετοχή τρίτων στη χρηματοδότηση 16
3.3. Εκτιμώμενες επιπτώσεις στα έσοδα 16

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

1.2. Σχετικοί τομείς πολιτικής *(ομάδα προγραμμάτων)*

Επικοινωνιακά Δίκτυα, Περιεχόμενο και Τεχνολογίες

1.3. Η πρόταση/πρωτοβουλία αφορά:

☐ **νέα δράση**

☐ **νέα δράση έπειτα από δοκιμαστικό σχέδιο / προπαρασκευαστική ενέργεια**[40]

☒ **την παράταση υφιστάμενης δράσης**

☐ **συγχώνευση ή αναπροσανατολισμό μίας ή περισσότερων δράσεων προς άλλη/νέα δράση**

1.4. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.4.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας

Στόχος της αναθεώρησης είναι να αυξηθεί το επίπεδο κυβερνοανθεκτικότητας ενός ολοκληρωμένου συνόλου επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς, να μειωθούν οι ασυνέπειες στην ανθεκτικότητα εντός της εσωτερικής αγοράς στους τομείς που καλύπτονται ήδη από την οδηγία και να βελτιωθεί το επίπεδο κοινής επίγνωσης της κατάστασης και η συλλογική ικανότητα προετοιμασίας και αντίδρασης.

1.4.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.

Η ανθεκτικότητα της κυβερνοασφάλειας σε ολόκληρη την Ένωση δεν μπορεί να είναι αποτελεσματική αν ακολουθείται ανομοιογενής προσέγγιση με εθνικά ή περιφερειακά στεγανά. Η οδηγία NIS ήρθε να καλύψει αυτήν την αδυναμία, καθορίζοντας ένα πλαίσιο για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων σε εθνικό και ενωσιακό επίπεδο. Ωστόσο, η πρώτη περιοδική επανεξέταση της οδηγίας NIS κατέδειξε ορισμένες εγγενείς αδυναμίες που έχουν οδηγήσει τελικά σε σημαντικές ανισότητες μεταξύ των κρατών μελών όσον αφορά τις ικανότητες, τον σχεδιασμό και το επίπεδο προστασίας, οι οποίες επηρεάζουν ταυτόχρονα τους ισότιμους όρους ανταγωνισμού για παρόμοιες εταιρείες στην εσωτερική αγορά.

Η παρέμβαση της ΕΕ που υπερβαίνει τα ισχύοντα μέτρα της οδηγίας NIS δικαιολογείται κυρίως από: i) τον διασυνοριακό χαρακτήρα του προβλήματος· ii) τις δυνατότητες της δράσης της ΕΕ για βελτίωση και διευκόλυνση αποτελεσματικών

[40] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχεία α) ή β) του δημοσιονομικού κανονισμού.

εθνικών πολιτικών· iii) τη συμβολή συντονισμένων και συνεργατικών δράσεων πολιτικής NIS στην αποτελεσματική προστασία των δεδομένων και της ιδιωτικής ζωής.

Οι δηλωμένοι στόχοι είναι, συνεπώς, δυνατό να επιτευχθούν καλύτερα μέσω δράσης σε επίπεδο ΕΕ, και όχι μεμονωμένα από τα κράτη μέλη.

1.4.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος

Η οδηγία NIS αποτελεί το πρώτο οριζόντιο μέσο εσωτερικής αγοράς που αποσκοπεί στη βελτίωση της ανθεκτικότητας των δικτύων και των συστημάτων στην Ένωση έναντι κινδύνων κυβερνοασφάλειας. Έχει ήδη συμβάλει σημαντικά στην αύξηση του κοινού επιπέδου κυβερνοασφάλειας μεταξύ των κρατών μελών. Ωστόσο, η επανεξέταση της λειτουργίας και της εφαρμογής της οδηγίας κατέδειξε ορισμένες αδυναμίες, οι οποίες, μαζί με την αυξανόμενη ψηφιοποίηση και την ανάγκη πιο επίκαιρης αντίδρασης, πρέπει να αντιμετωπιστούν με αναθεωρημένη νομική πράξη.

1.4.4. Συμβατότητα και ενδεχόμενη συνέργεια με άλλα κατάλληλα μέσα

Η νέα πρόταση είναι πλήρως συνεπής και συνεκτική με άλλες συναφείς πρωτοβουλίες, όπως η πρόταση κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA) και η πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων φορέων εκμετάλλευσης βασικών υπηρεσιών. Είναι επίσης συνεπής προς τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών, τον Γενικό Κανονισμό για την Προστασία Δεδομένων και τον κανονισμό eIDAS.

Η πρόταση αποτελεί βασικό μέρος της στρατηγικής της ΕΕ για την Ένωση Ασφάλειας.

1.5. Διάρκεια και δημοσιονομικές επιπτώσεις

☐ **περιορισμένη διάρκεια**

– ☐ με ισχύ από [HH/MM]EEEE έως [HH/MM]EEEE

– ☐ Δημοσιονομικές επιπτώσεις από το EEEE έως το EEEE για πιστώσεις αναλήψεων υποχρεώσεων και από το EEEE έως το EEEE για πιστώσεις πληρωμών.

☒ **απεριόριστη διάρκεια**

– Περίοδος σταδιακής εφαρμογής από το 2022 έως το 2025

– και στη συνέχεια πλήρης εφαρμογή.

1.6. Προβλεπόμενοι τρόποι διαχείρισης[41]

Άμεση διαχείριση από την Επιτροπή

– ☒ από τις υπηρεσίες της, συμπεριλαμβανομένου του προσωπικού της στις αντιπροσωπείες της Ένωσης

– ☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☐ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

– ☐ σε τρίτες χώρες ή οργανισμούς που αυτές έχουν ορίσει

– ☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)

– ☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων

– Χ☐ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71 του δημοσιονομικού κανονισμού

– ☐ σε οργανισμούς δημοσίου δικαίου

– ☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις

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

– ☐ σε πρόσωπα επιφορτισμένα με την εφαρμογή συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη

– *Αν αναφέρονται περισσότεροι του ενός τρόποι διαχείρισης, να διευκρινιστούν στο τμήμα «Παρατηρήσεις».*

Παρατηρήσεις

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, στον οποίο έχει ανατεθεί νέα μόνιμη εντολή με την πράξη για την κυβερνοασφάλεια, θα συνδράμει τα κράτη μέλη και την Επιτροπή στην εφαρμογή της αναθεωρημένης οδηγίας NIS.

[41] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης, καθώς και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον ιστότοπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EL/man/budgmanag/Pages/budgmanag.aspx

Ως αποτέλεσμα της αναθεωρημένης οδηγίας NIS, από το 2022/23, ο ENISA θα διαθέτει πρόσθετους τομείς δράσης. Αν και αυτοί οι τομείς δράσης θα καλύπτονται από τα γενικά καθήκοντα του ENISA σύμφωνα με την εντολή του, θα έχουν ως αποτέλεσμα πρόσθετο φόρτο εργασίας για τον οργανισμό. Πιο συγκεκριμένα, εκτός από τους τρέχοντες τομείς δράσης του, βάσει της πρότασης της Επιτροπής για αναθεωρημένη οδηγία NIS, θα απαιτηθεί επίσης από τον ENISA να ενσωματώσει ειδικά στο πρόγραμμα εργασίας του, μεταξύ άλλων, τις ακόλουθες δράσεις: i) ανάπτυξη και τήρηση ευρωπαϊκού μητρώου τρωτών σημείων (άρθρο 6 παράγραφος 2 της πρότασης), ii) παροχή γραμματειακής υποστήριξης στο ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (CyCLONe) (άρθρο 14 της πρότασης) και έκδοση ετήσιας έκθεσης σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ (άρθρο 15 της πρότασης), iii) υποστήριξη της διοργάνωσης αξιολογήσεων από ομοτίμους μεταξύ των κρατών μελών (άρθρο 16 της πρότασης), iv) συλλογή συγκεντρωτικών δεδομένων περιστατικών από τα κράτη μέλη και έκδοση τεχνικής καθοδήγησης (άρθρο 20 παράγραφος 9 της πρότασης), v) δημιουργία και τήρηση μητρώου για οντότητες που παρέχουν διασυνοριακές υπηρεσίες (άρθρο 25 της πρότασης).

Κατά συνέπεια, θα υποβληθεί αίτημα για 5 συμπληρωματικά ΙΠΑ από το 2022, καθώς και για τον αντίστοιχο προϋπολογισμό ύψους περίπου 0,61 εκατ. EUR ετησίως για την κάλυψη αυτών των νέων θέσεων (βλ. χωριστό δημοσιονομικό δελτίο για τους οργανισμούς).

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι.

Η Επιτροπή θα επανεξετάζει περιοδικά τη λειτουργία της οδηγίας και θα υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, την πρώτη φορά τρία έτη μετά την έναρξη ισχύος της. Η Επιτροπή θα αξιολογήσει επίσης την ορθή μεταφορά της οδηγίας από τα κράτη μέλη.

2.2. Συστήματα διαχείρισης και ελέγχου

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου

Η Διοικητική Μονάδα εντός της ΓΔ CNECT που είναι αρμόδια για τον τομέα πολιτικής θα διαχειρίζεται την εφαρμογή της οδηγίας.

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους

Πολύ χαμηλός κίνδυνος, δεδομένου ότι το οικοσύστημα της οδηγίας NIS υφίσταται ήδη.

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)

Άνευ αντικειμένου. Χρησιμοποίηση μόνο διοικητικού προϋπολογισμού («συνολικό κονδύλιο»).

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.

Άνευ αντικειμένου. Χρησιμοποίηση μόνο διοικητικού προϋπολογισμού («συνολικό κονδύλιο»).

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και νέες γραμμές δαπανών του προϋπολογισμού που προτείνονται

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός [Τομέας…7……...……]	ΔΠ/ΜΔΠ[42]	χωρών ΕΖΕΣ[43]	υποψηφίων για ένταξη χωρών[44]	τρίτων χωρών	κατά την έννοια του άρθρου[21 παράγραφος 2 στοιχείο β)] του δημοσιονομικού κανονισμού
	20 02 06 διαχειριστικές δαπάνες 20 02 06	ΜΔΠ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

[42] ΔΠ = Διαχωριζόμενες πιστώσεις / ΜΔΠ = Μη διαχωριζόμενες πιστώσεις.

[43] ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

[44] Υποψήφιες χώρες και, κατά περίπτωση, δυνάμει υποψήφια μέλη της ΕΕ από τα Δυτικά Βαλκάνια.

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου	**<…>**	[Τομέας ……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Μετά το 2027***	**ΣΥΝΟΛΟ**
Επιχειρησιακές πιστώσεις (κατανεμημένες σύμφωνα με τις γραμμές του προϋπολογισμού στο σημείο 3.1)	Αναλήψεις υποχρεώσεων	(1)									
	Πληρωμές	(2)									
Πιστώσεις διοικητικού χαρακτήρα χρηματοδοτούμενες από το κονδύλιο του προγράμματος[45]	Αναλήψεις υποχρεώσεων = Πληρωμές	(3)									
ΣΥΝΟΛΟ πιστώσεων για το χρηματοδοτικό κονδύλιο του προγράμματος	Αναλήψεις υποχρεώσεων	=1+3									
	Πληρωμές	=2+3									

Τομέας του πολυετούς δημοσιονομικού πλαισίου	7	«Διοικητικές δαπάνες» Συνεδριάσεις: οι συνεδριάσεις ολομέλειας της ομάδας συνεργασίας NIS πραγματοποιούνται συνήθως 4 φορές ανά έτος. Η Επιτροπή καλύπτει τις δαπάνες τροφοδοσίας και τα έξοδα ταξιδίου των εκπροσώπων 27 κρατών μελών (ένας εκπρόσωπος ανά κράτος μέλος). Το κόστος μιας συνεδρίασης θα μπορούσε να ανέλθει έως και στο ποσό των 15 EUR.

[45] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

		Αποστολές: οι αποστολές σχετίζονται με την παρακολούθηση της εφαρμογής της οδηγίας NIS. Παράδειγμα: Σε ένα έτος (Μάιος 2019 – Ιούλιος 2020) επρόκειτο να διοργανώσουμε τις λεγόμενες «επισκέψεις χώρας NIS» και να επισκεφθούμε και τα 27 κράτη μέλη για να συζητήσουμε την εφαρμογή της οδηγίας NIS σε ολόκληρη την ΕΕ.

Αυτό το τμήμα πρέπει να συμπληρωθεί με «στοιχεία διοικητικού χαρακτήρα του προϋπολογισμού» τα οποία θα εισαχθούν, πρώτα, στο παράρτημα του νομοθετικού δημοσιονομικού δελτίου, που τηλεφορτώνεται στο DECIDE για διυπηρεσιακή διαβούλευση.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		2021	2022	2023	2024	2025	2026	2027	*Μετά το 2027*	ΣΥΝΟΛΟ
Ανθρώπινοι πόροι		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Άλλες διοικητικές δαπάνες		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		2021	2022	2023	2024	2025	2026	2027	*Μετά το 2027*	ΣΥΝΟΛΟ
ΣΥΝΟΛΟ πιστώσεων μεταξύ ΤΟΜΕΩΝ του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων									
	Πληρωμές									

3.2.2. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις πιστώσεις διοικητικού χαρακτήρα

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

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

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Έτη	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**ΣΥΝΟΛΟ**
ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου								
Ανθρώπινοι πόροι	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Άλλες διοικητικές δαπάνες	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**
Εκτός του ΤΟΜΕΑ 7[46] του πολυετούς δημοσιονομικού πλαισίου								
Ανθρώπινοι πόροι								
Άλλες δαπάνες διοικητικού χαρακτήρα								
Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου								
ΣΥΝΟΛΟ	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Οι απαιτούμενες πιστώσεις για ανθρώπινους πόρους και άλλες δαπάνες διοικητικού χαρακτήρα θα καλυφθούν από τις πιστώσεις της ΓΔ που έχουν ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχουν ανακατανεμηθεί στο εσωτερικό της ΓΔ, οι οποίες θα συμπληρωθούν, αν χρειαστεί, με τυχόν πρόσθετα κονδύλια που μπορεί να χορηγηθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

[46] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

3.2.2.1. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους

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

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

Εκτίμηση η οποία πρέπει να εκφράζεται σε μονάδες ισοδυνάμων πλήρους απασχόλησης

Έτη		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)								
Έδρα και αντιπροσωπείες της Επιτροπής		6	6	6	6	6	6	6
Αντιπροσωπείες της ΕΕ								
Έρευνα								
• Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ) — AC, AL, END, INT και JED [47] Τομέας 7								
Χρηματοδοτούμενο από τον ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	– στην έδρα:	3	3	3	3	3	3	3
	- στις αντιπροσωπείες της ΕΕ							
Χρηματοδοτούμενο από το κονδύλιο του προγράμματος [48]	– στην έδρα:							
	- στις αντιπροσωπείες της ΕΕ							
Έρευνα								
Άλλο (να προσδιοριστεί)								
ΣΥΝΟΛΟ		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	• προετοιμασία κατ' εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 18 παράγραφος 6, το άρθρο 21 παράγραφος 2 και το άρθρο 36· • προετοιμασία εκτελεστικών πράξεων σύμφωνα με το άρθρο 12 παράγραφος 8, το άρθρο 18 παράγραφος 5 και το άρθρο 20 παράγραφος 11· • γραμματειακή υποστήριξη της ομάδας συνεργασίας NIS· • διοργάνωση συνεδριάσεων της ολομέλειας και των αξόνων εργασίας της ομάδας συνεργασίας NIS· • συντονισμός εργασιών των κρατών μελών για διάφορα έγγραφα (κατευθυντήριες γραμμές, εργαλειοθήκες κ.λπ.)· • διασύνδεση με άλλες υπηρεσίες της Επιτροπής, τον ENISA και τις εθνικές αρχές με σκοπό την εφαρμογή της οδηγίας NIS· • ανάλυση εθνικών μεθόδων και βέλτιστων πρακτικών σχετικών με την εφαρμογή της οδηγίας NIS.

[47] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

[48] Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

Εξωτερικό προσωπικό	υποστήριξη όλων των ανωτέρω καθηκόντων κατά περίπτωση

3.2.3. Συμμετοχή τρίτων στη χρηματοδότηση

Η πρόταση/πρωτοβουλία:

– Χ☐ δεν προβλέπει συγχρηματοδότηση από τρίτους

– ☐ προβλέπει τη συγχρηματοδότηση από τρίτους που εκτιμάται κατωτέρω:

Πιστώσεις σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Έτη	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**ΣΥΝΟΛΟ**
Προσδιορισμός του φορέα συγχρηματοδότησης								
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων								

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

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

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

☐ στους ιδίους πόρους

☐ στα λοιπά έσοδα

Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών ☐

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Γραμμή εσόδων του προϋπολογισμού:	Επιπτώσεις της πρότασης/πρωτοβουλίας[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Άρθρο …….							

Ως προς τα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

Άλλες παρατηρήσεις (π.χ. μέθοδος/τύπος για τον υπολογισμό των επιπτώσεων στα έσοδα ή τυχόν άλλες πληροφορίες).

[49] Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.

ΠΑΡΑΡΤΗΜΑ
του ΝΟΜΟΘΕΤΙΚΟΥ ΔΗΜΟΣΙΟΝΟΜΙΚΟΥ ΔΕΛΤΙΟΥ

Τίτλος της πρότασης/πρωτοβουλίας:

Πρόταση οδηγίας για την αναθεώρηση της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας δικτυακών και πληροφοριακών συστημάτων σε ολόκληρη την Ένωση

……
……

1. ΑΡΙΘΜΟΣ και ΚΟΣΤΟΣ των ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ ΠΟΥ ΚΡΙΝΟΝΤΑΙ ΑΠΑΡΑΙΤΗΤΟΙ

2. ΚΟΣΤΟΣ ΑΛΛΩΝ ΔΙΟΙΚΗΤΙΚΩΝ ΔΑΠΑΝΩΝ

3. ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΕΣ ΜΕΘΟΔΟΙ ΥΠΟΛΟΓΙΣΜΟΥ ΓΙΑ ΤΗΝ ΕΚΤΙΜΗΣΗ ΤΟΥ ΚΟΣΤΟΥΣ

3.1 Ανθρώπινοι πόροι

3.2 Άλλες διοικητικές δαπάνες

*Το παρόν παράρτημα, **το οποίο συμπληρώνεται από κάθε ΓΔ/Υπηρεσία που συμμετέχει στην πρόταση/πρωτοβουλία**, πρέπει να συνοδεύει το νομοθετικό δημοσιονομικό δελτίο κατά την έναρξη της διαβούλευσης μεταξύ των υπηρεσιών.*

Οι πίνακες δεδομένων χρησιμοποιούνται ως πηγή για τους πίνακες που περιλαμβάνονται στο νομοθετικό δημοσιονομικό δελτίο. Προορίζονται αποκλειστικά για εσωτερική χρήση στο πλαίσιο της Επιτροπής.

1. Κόστος των ανθρώπινων πόρων που κρίνονται απαραίτητοι

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

X☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**ΣΥΝΟΛΟ**	
		ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις
• Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)																	
Έδρα και αντιπροσωπείες της Επιτροπής	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
σε αντιπροσωπείες της Ένωσης	AD																
	AST																
• Εξωτερικό προσωπικό [50] 0,24																	
Συνολικό κονδύλιο	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	END																
	INT																
σε αντιπροσωπείες της Ένωσης	AC																
	AL																

[50] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

	END																
	INT																
	JPD																
Άλλες γραμμές του προϋπολογισμού (*να προσδιοριστούν*)																	
Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου			2021		2022		2023		2024		2025		2025		2025		ΣΥΝΟΛΟ	
			ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις	ΙΠΑ	Πιστώσεις
• Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)																		
Έρευνα		AD																
		AST																
• Εξωτερικό προσωπικό [51]																		
Εξωτερικό προσωπικό που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).	- στην έδρα	AC																
		END																
		INT																
	- Σε αντιπροσωπίες της Ένωσης	AC																
		AL																
		END																
		INT																
		JPD																
Έρευνα)		AC																
		END																
		INT																

[51] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

Άλλες γραμμές του προϋπολογισμού (*να προσδιοριστούν*)																	
Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου																	

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Εκτιμώμενες επιπτώσεις στο ανθρώπινο δυναμικό του ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, στον οποίο έχει ανατεθεί νέα μόνιμη εντολή με την πράξη για την κυβερνοασφάλεια, θα συνδράμει τα κράτη μέλη και την Επιτροπή στην εφαρμογή της αναθεωρημένης οδηγίας NIS.

Ως αποτέλεσμα της αναθεωρημένης οδηγίας NIS, από το 2022/23, ο ENISA θα διαθέτει πρόσθετους τομείς δράσης. Αν και αυτοί οι τομείς δράσης θα καλύπτονται από τα γενικά καθήκοντα του ENISA σύμφωνα με την εντολή του, θα έχουν ως αποτέλεσμα πρόσθετο φόρτο εργασίας για τον οργανισμό. Πιο συγκεκριμένα, εκτός από τους τρέχοντες τομείς δράσης του, βάσει της πρότασης της Επιτροπής για αναθεωρημένη οδηγία NIS, θα απαιτηθεί επίσης από τον ENISA να ενσωματώσει ειδικά στο πρόγραμμα εργασίας του, μεταξύ άλλων, τις ακόλουθες δράσεις: i) ανάπτυξη και τήρηση ευρωπαϊκού μητρώου τρωτών σημείων (άρθρο 6 παράγραφος 2 της πρότασης), ii) παροχή γραμματειακής υποστήριξης στο ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (CyCLONe) (άρθρο 14 της πρότασης) και έκδοση ετήσιας έκθεσης σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ (άρθρο 15 της πρότασης), iii) υποστήριξη της διοργάνωσης αξιολογήσεων από ομοτίμους μεταξύ των κρατών μελών (άρθρο 16 της πρότασης), iv) συλλογή συγκεντρωτικών δεδομένων περιστατικών από τα κράτη μέλη και έκδοση τεχνικής καθοδήγησης (άρθρο 20 παράγραφος 9 της πρότασης), v) δημιουργία και τήρηση μητρώου για οντότητες που παρέχουν διασυνοριακές υπηρεσίες (άρθρο 25 της πρότασης).

Κατά συνέπεια, θα υποβληθεί αίτημα για 5 συμπληρωματικά ΙΠΑ από το 2022, καθώς και για τον αντίστοιχο προϋπολογισμό ύψους περίπου 0,61 εκατ. EUR ετησίως για την κάλυψη αυτών των νέων θέσεων (βλ. χωριστό δημοσιονομικό δελτίο για τους οργανισμούς).

Κατά συνέπεια, θα υποβληθεί αίτημα για 5 συμπληρωματικά ΙΠΑ από το 2022, καθώς και για τον αντίστοιχο προϋπολογισμό για την κάλυψη αυτών των νέων θέσεων.

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

☐X Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

	Έτος **N** [52] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)	**ΣΥΝΟΛΟ**

[52] Το έτος N είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «N» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

Έκτακτοι υπάλληλοι (βαθμοί AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Έκτακτοι υπάλληλοι (βαθμοί AST)								
Συμβασιούχοι υπάλληλοι	0,160	0,160	0,160	0,160	0,160	0,160		
Αποσπασμένοι εθνικοί εμπειρογνώμονες								**0,96**

ΣΥΝΟΛΟ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Απαιτήσεις προσωπικού (ΙΠΑ):

	Έτος **N** [53] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)			**ΣΥΝΟΛΟ**
Έκτακτοι υπάλληλοι (βαθμοί AD)	3	3	3	3	3	3		**18**
Έκτακτοι υπάλληλοι (βαθμοί AST)								
Συμβασιούχοι υπάλληλοι	2	2	2	2	2	2		**12**

[53] Το έτος N είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «N» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

Αποσπασμένοι εθνικοί εμπειρογνώμονες								
ΣΥΝΟΛΟ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Κόστος άλλων διοικητικών δαπανών

☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση διοικητικών πιστώσεων

X☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση διοικητικών πιστώσεων, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Σύνολο**
στην έδρα:								
Έξοδα αποστολών και παράστασης	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Έξοδα διασκέψεων και συνεδριάσεων	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Επιτροπές[54]								
Μελέτες και διαβουλεύσεις								

[54] Να προσδιοριστούν το είδος της επιτροπής και η ομάδα στην οποία ανήκει.

Συστήματα πληροφοριών και διαχείρισης								
Εξοπλισμός και υπηρεσίες ΤΠΕ[55]								
Άλλες γραμμές του προϋπολογισμού (*να προσδιοριστούν κατά περίπτωση*)								
Σε αντιπροσωπίες της Ένωσης								
Έξοδα αποστολών, διασκέψεων και παράστασης								
Περαιτέρω επαγγελματική επιμόρφωση προσωπικού								
Απόκτηση, μίσθωση και συναφείς δαπάνες								
Εξοπλισμός, έπιπλα, προμήθειες και υπηρεσίες								
Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] ΤΠΕ: Τεχνολογίες πληροφοριών και επικοινωνιών: πρέπει να ζητείται η γνώμη της DIGIT.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Σύνολο**
Δαπάνες τεχνικής και διοικητικής βοήθειας (μη συμπεριλαμβανομένου του εξωτερικού προσωπικού) βάσει επιχειρησιακών πιστώσεων (πρώην γραμμές «ΒΑ»)								
- στην έδρα								
- Σε αντιπροσωπίες της Ένωσης								
Άλλες διαχειριστικές δαπάνες για έρευνα								
Άλλες γραμμές του προϋπολογισμού (*να προσδιοριστούν κατά περίπτωση*)								
Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου								

ΣΥΝΟΛΟ **του ΤΟΜΕΑ 7 και εκτός του ΤΟΜΕΑ 7** του πολυετούς δημοσιονομικού πλαισίου	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Οι απαιτούμενες διοικητικές πιστώσεις θα καλυφθούν από τις πιστώσεις που έχουν ήδη διατεθεί για τη διαχείριση της δράσης και/ή που έχουν ανακατανεμηθεί στο εσωτερικό της ΓΔ και θα συμπληρωθούν, εάν χρειαστεί, με πρόσθετα κονδύλια που ενδέχεται να χορηγηθούν στην αρμόδια για τη διαχείριση της δράσης ΓΔ, στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

3. Χρησιμοποιούμενες μέθοδοι υπολογισμού για την εκτίμηση του κόστους

3,1 Ανθρώπινοι πόροι

Στο παρόν τμήμα καθορίζεται η χρησιμοποιούμενη μέθοδος υπολογισμού για την εκτίμηση των ανθρώπινων πόρων που θεωρούνται απαραίτητοι [παραδοχές φόρτου εργασίας, συμπεριλαμβανομένων των ειδικών θέσεων εργασίας (προφίλ εργασιών του συστήματος διαχείρισης προσωπικού SYSPER 2), των κατηγοριών προσωπικού και του αντίστοιχου μέσου κόστους]

ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου
ΣΗΜ.: Το μέσο κόστος για κάθε κατηγορία προσωπικού στην έδρα είναι διαθέσιμο στον ιστότοπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EL/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Μόνιμοι και έκτακτοι υπάλληλοι 6 υπάλληλοι σε ΙΠΑ (μέσο κόστος 0,150) = 0,9 ανά έτος - προετοιμασία κατ' εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 18 παράγραφος 6, το άρθρο 21 παράγραφος 2 και το άρθρο 36· - προετοιμασία εκτελεστικών πράξεων σύμφωνα με το άρθρο 12 παράγραφος 8, το άρθρο 18 παράγραφος 5 και το άρθρο 20 παράγραφος 11· - γραμματειακή υποστήριξη της ομάδας συνεργασίας NIS· - διοργάνωση συνεδριάσεων της ολομέλειας και των αξόνων εργασίας της ομάδας συνεργασίας NIS· - συντονισμός εργασιών των κρατών μελών για διάφορα έγγραφα (κατευθυντήριες γραμμές, εργαλειοθήκες κ.λπ.)· - διασύνδεση με άλλες υπηρεσίες της Επιτροπής, τον ENISA και τις εθνικές αρχές με σκοπό την εφαρμογή της οδηγίας NIS· - ανάλυση εθνικών μεθόδων και βέλτιστων πρακτικών σχετικών με την εφαρμογή της οδηγίας NIS.
• Εξωτερικό προσωπικό 3 AC (μέσο κόστος 0,08) = 0,24 ανά έτος - υποστήριξη όλων των ανωτέρω καθηκόντων κατά περίπτωση

Εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου
• Μόνον οι θέσεις που χρηματοδοτούνται από τον προϋπολογισμό για την έρευνα
• Εξωτερικό προσωπικό

3,2 Άλλες διοικητικές δαπάνες

Να αναφερθεί λεπτομερώς η χρησιμοποιούμενη μέθοδος υπολογισμού για κάθε γραμμή του προϋπολογισμού και να προσδιοριστούν ειδικότερα οι υποκείμενες παραδοχές (π.χ. αριθμός συνεδριάσεων ετησίως, μέσο κόστος κ.λπ.)

ΤΟΜΕΑΣ 7 του πολυετούς δημοσιονομικού πλαισίου

Συνεδριάσεις: οι συνεδριάσεις ολομέλειας της ομάδας συνεργασίας NIS πραγματοποιούνται συνήθως 4 φορές ανά έτος. Η Επιτροπή καλύπτει τις δαπάνες τροφοδοσίας και τα έξοδα ταξιδίου των εκπροσώπων 27 κρατών μελών (ένας εκπρόσωπος ανά κράτος μέλος). Το κόστος μίας συνεδρίασης είναι δυνατό να ανέλθει σε 15 000 EUR, άρα το αθροιστικό κόστος ανέρχεται σε 60 000 EUR ετησίως.

Αποστολές: οι αποστολές σχετίζονται με την παρακολούθηση της εφαρμογής της οδηγίας NIS. Παράδειγμα: Σε ένα έτος (Μάιος 2019 – Ιούλιος 2020) επρόκειτο να διοργανώσουμε τις λεγόμενες «επισκέψεις χώρας NIS» και να επισκεφθούμε και τα 27 κράτη μέλη για να συζητήσουμε

την εφαρμογή της οδηγίας NIS σε ολόκληρη την ΕΕ.

Εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου

ΠΑΡΑΡΤΗΜΑ 7

της
ΑΠΟΦΑΣΗΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

σχετικά με τους εσωτερικούς κανόνες για την εκτέλεση του γενικού προϋπολογισμού της Ευρωπαϊκής Ένωσης (τμήμα Ευρωπαϊκή Επιτροπή) υπόψη των υπηρεσιών της Επιτροπής

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ «ΟΡΓΑΝΙΣΜΟΙ»

Το παρόν ΝΔΔ καλύπτει το αίτημα για αύξηση του προσωπικού του ENISA κατά 5 ΙΠΑ από το 2022 για την εκτέλεση συμπληρωματικών δραστηριοτήτων που συνδέονται με την εφαρμογή της οδηγίας NIS. Οι δραστηριότητες αυτές ήδη καλύπτονται από την εντολή του ENISA.

Περιεχόμενα

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ 19

1.1. Τίτλος της πρότασης/πρωτοβουλίας 19

1.2. Σχετικοί τομείς πολιτικής 19

1.3. Η πρόταση αφορά 19

1.4. Στόχοι 19

1.4.1. Γενικοί στόχοι 19

1.4.2. Ειδικοί στόχοι 19

1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις 21

1.4.4. Δείκτες επιδόσεων 22

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας 23

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας 23

1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα. 23

1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος 23

1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα 24

1.5.5. Αξιολόγηση των διάφορων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής 24

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας 25

1.7. Προβλεπόμενοι τρόποι διαχείρισης 25

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ 27

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων 27

2.2. Συστήματα διαχείρισης και ελέγχου 27

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου 27

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους 27

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο) 28

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας 29

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ 29
3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται 29
3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες 31
3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες 31
3.2.2. Εκτιμώμενες επιπτώσεις στις πιστώσεις [του οργανισμού] 34
3.2.3. Εκτιμώμενες επιπτώσεις στο ανθρώπινο δυναμικό του ENISA 36
3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο 39
3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση 39
3.3. Εκτιμώμενες επιπτώσεις στα έσοδα 40

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

1.2. Σχετικοί τομείς πολιτικής

Επικοινωνιακά Δίκτυα, Περιεχόμενο και Τεχνολογίες

1.3. Η πρόταση αφορά

☐ **νέα δράση**

☐ **νέα δράση έπειτα από δοκιμαστικό σχέδιο / προπαρασκευαστική ενέργεια**[56]

☒ **την παράταση υφιστάμενης δράσης**

☐ **συγχώνευση μίας ή περισσότερων δράσεων προς άλλη/νέα δράση**

1.4. Στόχοι

1.4.1. Γενικοί στόχοι

Στόχος της αναθεώρησης είναι να αυξηθεί το επίπεδο κυβερνοανθεκτικότητας ενός ολοκληρωμένου συνόλου επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς, να μειωθούν οι ασυνέπειες στην ανθεκτικότητα εντός της εσωτερικής αγοράς στους τομείς που καλύπτονται ήδη από την οδηγία και να βελτιωθεί το επίπεδο κοινής επίγνωσης της κατάστασης και η συλλογική ικανότητα προετοιμασίας και αντίδρασης.

1.4.2. Ειδικοί στόχοι

Για να αντιμετωπιστεί το πρόβλημα του χαμηλού επιπέδου κυβερνοανθεκτικότητας των επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση, ο ειδικός στόχος είναι να διασφαλιστεί ότι οι οντότητες σε όλους τους τομείς που εξαρτώνται από δικτυακά και πληροφοριακά συστήματα και παρέχουν βασικές υπηρεσίες στην οικονομία και την κοινωνία συνολικά υποχρεούνται να λαμβάνουν μέτρα κυβερνοασφάλειας και να αναφέρουν περιστατικά με σκοπό την αύξηση του συνολικού επιπέδου κυβερνοανθεκτικότητας σε ολόκληρη την εσωτερική αγορά.

Για να αντιμετωπιστεί το πρόβλημα των διαφορών όσον αφορά την ανθεκτικότητα μεταξύ κρατών μελών και τομέων, ο ειδικός στόχος είναι να διασφαλιστεί ότι όλες οι οντότητες οι οποίες δραστηριοποιούνται σε τομείς που καλύπτονται από το νομικό πλαίσιο NIS και οι οποίες είναι παρόμοιου μεγέθους και έχουν συγκρίσιμο ρόλο υπόκεινται στο ίδιο ρυθμιστικό καθεστώς (είτε εμπίπτουν στο πεδίο εφαρμογής είτε όχι), ανεξάρτητα από τη δικαιοδοσία στην οποία υπάγονται εντός της ΕΕ.

Για να διασφαλιστεί ότι όλες οι οντότητες οι οποίες δραστηριοποιούνται σε τομείς που καλύπτονται από το νομικό πλαίσιο NIS πρέπει να τηρούν τις ίδιες υποχρεώσεις με βάση την έννοια της διαχείρισης κινδύνου όσον αφορά τα μέτρα ασφάλειας και να αναφέρουν όλα τα

[56] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχεία α) ή β) του δημοσιονομικού κανονισμού.

περιστατικά βάσει ενιαίου συνόλου κριτηρίων, οι ειδικοί στόχοι είναι να διασφαλιστεί ότι οι αρμόδιες αρχές εφαρμόζουν αποτελεσματικότερα τους κανόνες που ορίζονται από τη νομική πράξη μέσω εναρμονισμένων μέτρων εποπτείας και επιβολής και να διασφαλιστεί συγκρίσιμο επίπεδο μεταξύ κρατών μελών όσον αφορά τους πόρους που διατίθενται στις αρμόδιες αρχές και θα τους παρέχουν τη δυνατότητα να εκπληρώνουν τα βασικά καθήκοντα τα οποία ορίζονται από το πλαίσιο NIS.

Για να αντιμετωπιστεί το πρόβλημα της κοινής επίγνωσης της κατάστασης και της έλλειψης κοινής αντιμετώπισης κρίσεων, ο ειδικός στόχος είναι να διασφαλιστεί η ανταλλαγή βασικών πληροφοριών μεταξύ κρατών μελών με την επιβολή στις αρμόδιες αρχές σαφών υποχρεώσεων ανταλλαγής πληροφοριών και συνεργασίας όταν πρόκειται για κυβερνοαπειλές και περιστατικά, καθώς και με την ανάπτυξη ενωσιακής κοινής επιχειρησιακής ικανότητας για την αντιμετώπιση κρίσεων.

1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις

Να προσδιοριστούν τα αποτελέσματα που αναμένεται να έχει η πρόταση/πρωτοβουλία όσον αφορά τους/τις στοχευόμενους/-ες δικαιούχους/ομάδες.

Η πρόταση αναμένεται να αποφέρει σημαντικά οφέλη: σύμφωνα με εκτιμήσεις, ενδέχεται να οδηγήσει σε μείωση του κόστους των περιστατικών κυβερνοασφάλειας κατά 11,3 δισ. EUR. Το τομεακό πεδίο εφαρμογής θα διευρυνθεί σημαντικά στο πλαίσιο NIS, ωστόσο, παράλληλα με τα ανωτέρω οφέλη, η επιβάρυνση που ενδέχεται να προκύψει από τις απαιτήσεις NIS, ιδίως από την πλευρά της επίβλεψης, θα είναι επίσης ισορροπημένη τόσο για τις νέες οντότητες που θα καλύπτονται όσο και για τις αρμόδιες αρχές. Αυτό οφείλεται στο ότι το νέο πλαίσιο NIS θα καθιερώσει προσέγγιση δύο επιπέδων, με έμφαση στις μεγάλες και βασικές οντότητες και διαφοροποίηση του εποπτικού καθεστώτος που επιτρέπει μόνο την εκ των υστέρων επίβλεψη για μεγάλο αριθμό εξ αυτών, ιδίως εκείνων που θεωρούνται «σημαντικές» αλλά όχι «βασικές».

Συνολικά, η πρόταση θα οδηγήσει σε αποδοτικές αντισταθμίσεις και συνέργειες, με τις βέλτιστες δυνατότητες από όλες τις επιλογές πολιτικής που αναλύθηκαν, ώστε να διασφαλιστεί αυξημένο και συνεκτικό επίπεδο κυβερνοανθεκτικότητας βασικών οντοτήτων σε ολόκληρη την Ένωση, το οποίο θα οδηγήσει εν τέλει σε εξοικονόμηση κόστους τόσο για τις επιχειρήσεις όσο και για την κοινωνία.

Από την πρόταση θα προκύψει επίσης ορισμένο κόστος συμμόρφωσης και επιβολής για τις αρμόδιες αρχές των κρατών μελών (εκτιμήθηκε συνολική αύξηση κατά περίπου 20-30 % των πόρων). Ωστόσο, το νέο πλαίσιο θα αποφέρει επίσης σημαντικά οφέλη μέσω καλύτερης επισκόπησης των βασικών επιχειρήσεων και αλληλεπίδρασης μαζί τους, ενισχυμένης διασυνοριακής επιχειρησιακής συνεργασίας, καθώς και μέσω αμοιβαίας συνδρομής και μηχανισμών αξιολόγησης από ομοτίμους. Τα οφέλη αυτά θα οδηγήσουν σε συνολική αύξηση των ικανοτήτων κυβερνοασφάλειας σε όλα τα κράτη μέλη.

Για τις εταιρείες που θα εμπίπτουν στο πεδίο εφαρμογής του πλαισίου NIS, εκτιμάται ότι θα χρειαστούν αύξηση των τρεχουσών δαπανών τους για την ασφάλεια ΤΠΕ κατά 22 % το πολύ για τα πρώτα έτη μετά τη θέσπιση του νέου πλαισίου NIS (το ποσοστό αυτό θα ανέρχεται σε 12 % για εταιρείες που εμπίπτουν ήδη στο πεδίο εφαρμογής της ισχύουσας οδηγίας NIS). Ωστόσο, αυτή η μέση αύξηση των δαπανών για την ασφάλεια ΤΠΕ θα οδηγήσει σε αναλογικό όφελος από τις εν λόγω επενδύσεις, ιδίως χάρη σε σημαντική μείωση του κόστους των περιστατικών κυβερνοασφάλειας (που εκτιμάται σε 118 δισ. EUR σε διάστημα δέκα ετών).

Οι μικρές και πολύ μικρές επιχειρήσεις θα εξαιρούνται από το πεδίο εφαρμογής του πλαισίου NIS. Για τις μεσαίες επιχειρήσεις, αναμένεται να σημειωθεί αύξηση του επιπέδου των δαπανών για την ασφάλεια ΤΠΕ κατά τα πρώτα έτη μετά τη θέσπιση του νέου πλαισίου NIS. Ταυτόχρονα, η αύξηση του επιπέδου των απαιτήσεων ασφάλειας για τις εν λόγω οντότητες θα παράσχει επίσης κίνητρα για τις οικείες ικανότητές κυβερνοασφάλειας και θα συμβάλει στη βελτίωση της οικείας διαχείρισης κινδύνου ΤΠΕ.

Θα υπάρξει επίπτωση στους εθνικούς προϋπολογισμούς και στις εθνικές διοικήσεις: βραχυπρόθεσμα και μεσοπρόθεσμα αναμένεται εκτιμώμενη αύξηση κατά περίπου 20-30 % των πόρων.

Δεν αναμένονται άλλες σημαντικές αρνητικές επιπτώσεις. Η πρόταση αναμένεται να οδηγήσει σε αρτιότερες ικανότητες κυβερνοασφάλειας και, κατά συνέπεια, θα έχει ουσιαστικότερες μετριαστικές επιπτώσεις στον αριθμό και τη σοβαρότητα των περιστατικών, συμπεριλαμβανομένων των παραβιάσεων δεδομένων. Είναι επίσης πιθανό η πρόταση να έχει

θετικές επιπτώσεις στη διασφάλιση ισότιμων όρων ανταγωνισμού σε όλα τα κράτη μέλη για όλες τις οντότητες που καλύπτονται από το πεδίο εφαρμογής της οδηγίας NIS και να μειώσει τις ασυμμετρίες πληροφόρησης στον τομέα της κυβερνοασφάλειας.

1.4.4. Δείκτες επιδόσεων

Να προσδιοριστούν οι δείκτες για την παρακολούθηση της προόδου και των επιτευγμάτων.

Η αξιολόγηση δεικτών θα διενεργείται από την Επιτροπή, με την υποστήριξη του ENISA και της ομάδας συνεργασίας, αρχής γενομένης τρία έτη μετά την έναρξη ισχύος της νέας νομικής πράξης NIS. Ορισμένοι από τους δείκτες παρακολούθησης βάσει των οποίων θα αξιολογηθεί η επιτυχία της επανεξέτασης της οδηγίας NIS είναι οι ακόλουθοι:

- Βελτιωμένος χειρισμός περιστατικών: με τη λήψη μέτρων κυβερνοασφάλειας, οι εταιρείες βελτιώνουν όχι μόνο την ικανότητά τους να αποφεύγουν εντελώς ορισμένα περιστατικά, αλλά και την ικανότητά τους για αντιμετώπιση περιστατικών. Επομένως, η επιτυχία μετράται με βάση i) τη μείωση του μέσου χρόνου που χρειάζεται για τον εντοπισμό ενός περιστατικού, ii) τον χρόνο που χρειάζονται κατά μέσο όρο οι οργανισμοί για αποκατάσταση από ένα περιστατικό και iii) το μέσο κόστος μιας ζημίας που προκλήθηκε από ένα περιστατικό.

- Αυξημένη επίγνωση των κινδύνων κυβερνοασφάλειας στα ανώτατα διοικητικά στελέχη των εταιρειών: απαιτώντας από τις εταιρείες να λάβουν μέτρα, η αναθεωρημένη οδηγία NIS θα συμβάλει στην αυξημένη επίγνωση των κινδύνων που σχετίζονται με την κυβερνοασφάλεια μεταξύ των ανώτατων διοικητικών στελεχών. Αυτός ο δείκτης μπορεί να μετρηθεί με τη μελέτη του βαθμού στον οποίο οι εταιρείες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS δίνουν προτεραιότητα στην κυβερνοασφάλεια για τις εσωτερικές εταιρικές πολιτικές και διαδικασίες, πρακτική που αποδεικνύεται από εσωτερική τεκμηρίωση, σχετικά προγράμματα κατάρτισης και δραστηριότητες ευαισθητοποίησης για τους εργαζομένους, ενώ δίνουν προτεραιότητα και σε επενδύσεις ΤΠΕ σχετικές με την ασφάλεια. Τα διοικητικά στελέχη όλων των βασικών και σημαντικών οντοτήτων θα πρέπει επίσης να έχουν επίγνωση των κανόνων που ορίζονται στην οδηγία NIS.

- Εξίσωση τομεακών δαπανών: οι δαπάνες για την ασφάλεια ΤΠΕ ποικίλλουν σημαντικά μεταξύ των τομέων στην ΕΕ. Με την απαίτηση λήψης μέτρων από τις εταιρείες σε περισσότερους τομείς, οι αποκλίσεις από τις μέσες τομεακές δαπάνες για την ασφάλεια ΤΠΕ ως ποσοστό των συνολικών δαπανών ΤΠΕ αναμένεται να ελαττωθούν μεταξύ τομέων και κρατών μελών.

- Ισχυρότερες αρμόδιες αρχές και αυξημένη συνεργασία: η αναθεωρημένη οδηγία NIS θα αναθέσει ενδεχομένως πρόσθετα καθήκοντα στις αρμόδιες αρχές. Αυτή η ανάθεση θα έχει μετρήσιμες επιπτώσεις στους οικονομικούς και ανθρώπινους πόρους που διατίθενται στους οργανισμούς κυβερνοασφάλειας σε εθνικό επίπεδο, ενώ αναμένεται επίσης να έχει θετικές επιπτώσεις στην ικανότητα των αρμόδιων αρχών να συνεργάζονται προορατικά και, ως εκ τούτου, να αυξήσει τον αριθμό των περιπτώσεων στις οποίες οι αρμόδιες αρχές συνεργάζονται μεταξύ τους με σκοπό την αντιμετώπιση διασυνοριακών περιστατικών ή την άσκηση κοινών εποπτικών δραστηριοτήτων.

- Αυξημένη ανταλλαγή πληροφοριών: η αναθεωρημένη οδηγία NIS θα βελτιώσει επίσης την ανταλλαγή πληροφοριών μεταξύ εταιρειών και με τις αρμόδιες αρχές. Ένας από τους στόχους της επανεξέτασης θα μπορούσε να είναι η αύξηση του αριθμού των οντοτήτων που συμμετέχουν στις διάφορες μορφές ανταλλαγής πληροφοριών.

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας

Στόχος της πρότασης είναι να αυξηθεί το επίπεδο κυβερνοανθεκτικότητας ενός ολοκληρωμένου συνόλου επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς, να μειωθούν οι ασυνέπειες στην ανθεκτικότητα εντός της εσωτερικής αγοράς στους τομείς που καλύπτονται ήδη από την οδηγία και να βελτιωθεί το επίπεδο κοινής επίγνωσης της κατάστασης και η συλλογική ικανότητα προετοιμασίας και αντίδρασης. Θα βασιστεί σε όσα έχουν επιτευχθεί με την εφαρμογή της οδηγίας (ΕΕ) 2016/1148 κατά τα 4 τελευταία έτη.

1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.

Η ανθεκτικότητα της κυβερνοασφάλειας σε ολόκληρη την Ένωση δεν μπορεί να είναι αποτελεσματική αν ακολουθείται ανομοιογενής προσέγγιση με εθνικά ή περιφερειακά στεγανά. Η οδηγία NIS ήρθε να καλύψει αυτήν την αδυναμία, καθορίζοντας ένα πλαίσιο για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων σε εθνικό και ενωσιακό επίπεδο. Ωστόσο, η πρώτη περιοδική επανεξέταση της οδηγίας NIS κατέδειξε ορισμένες εγγενείς αδυναμίες που έχουν οδηγήσει τελικά σε σημαντικές ανισότητες μεταξύ των κρατών μελών όσον αφορά τις ικανότητες, τον σχεδιασμό και το επίπεδο προστασίας, οι οποίες επηρεάζουν ταυτόχρονα τους ισότιμους όρους ανταγωνισμού για παρόμοιες εταιρείες στην εσωτερική αγορά.

Η παρέμβαση της ΕΕ που υπερβαίνει τα ισχύοντα μέτρα της οδηγίας NIS δικαιολογείται κυρίως από: i) τον διασυνοριακό χαρακτήρα του προβλήματος· ii) τις δυνατότητες της δράσης της ΕΕ για βελτίωση και διευκόλυνση αποτελεσματικών εθνικών πολιτικών· iii) τη συμβολή συντονισμένων και συνεργατικών δράσεων πολιτικής NIS στην αποτελεσματική προστασία των δεδομένων και της ιδιωτικής ζωής.

Οι δηλωμένοι στόχοι είναι, συνεπώς, δυνατό να επιτευχθούν καλύτερα μέσω δράσης σε επίπεδο ΕΕ, και όχι μεμονωμένα από τα κράτη μέλη.

1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος

Η οδηγία NIS αποτελεί το πρώτο οριζόντιο μέσο εσωτερικής αγοράς που αποσκοπεί στη βελτίωση της ανθεκτικότητας των δικτύων και των συστημάτων στην Ένωση έναντι κινδύνων κυβερνοασφάλειας. Από την έναρξη ισχύος της το 2016, έχει ήδη συμβάλει σημαντικά στην αύξηση του κοινού επιπέδου κυβερνοασφάλειας μεταξύ των κρατών μελών. Ωστόσο, η επανεξέταση της λειτουργίας και της εφαρμογής της οδηγίας κατέδειξε ορισμένες αδυναμίες, οι οποίες, μαζί με την αυξανόμενη ψηφιοποίηση και την ανάγκη πιο επίκαιρης αντίδρασης, πρέπει να αντιμετωπιστούν με αναθεωρημένη νομική πράξη.

1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα

Η νέα πρόταση είναι πλήρως συνεπής και συνεκτική με άλλες συναφείς πρωτοβουλίες, όπως η πρόταση κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA) και η πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων φορέων εκμετάλλευσης βασικών υπηρεσιών. Είναι επίσης συνεπής προς τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών, τον Γενικό Κανονισμό για την Προστασία Δεδομένων και τον κανονισμό eIDAS.

Η πρόταση αποτελεί βασικό μέρος της στρατηγικής της ΕΕ για την Ένωση Ασφάλειας.

1.5.5. Αξιολόγηση των διάφορων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής

Για τη διαχείριση αυτών των καθηκόντων από τον ENISA απαιτούνται ειδικά προφίλ και συμπληρωματικός φόρτος εργασίας που δεν είναι δυνατό να απορροφηθεί χωρίς αύξηση των ανθρώπινων πόρων.

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

☐ **περιορισμένη διάρκεια**

– ☐ Πρόταση/πρωτοβουλία με ισχύ από [ΗΗ/ΜΜ]ΕΕΕΕ έως [ΗΗ/ΜΜ]ΕΕΕΕ

– ☐ Δημοσιονομικές επιπτώσεις από το ΕΕΕΕ έως το ΕΕΕΕ

☒ **απεριόριστη διάρκεια**

– Περίοδος σταδιακής εφαρμογής από το 2022 έως το 2025

– και στη συνέχεια πλήρης εφαρμογή.

1.7. Προβλεπόμενοι τρόποι διαχείρισης[57]

☒ **Άμεση διαχείριση** από την Επιτροπή

μέσω

– ☐ εκτελεστικών οργανισμών

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☐Χ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)

☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων

☒ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71

☐ σε οργανισμούς δημοσίου δικαίου

☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις

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

☐ σε πρόσωπα επιφορτισμένα με την εφαρμογή συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη

Παρατηρήσεις

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, στον οποίο έχει ανατεθεί νέα μόνιμη εντολή με την πράξη για την κυβερνοασφάλεια, θα συνδράμει τα κράτη μέλη και την Επιτροπή στην εφαρμογή της αναθεωρημένης οδηγίας NIS.

Ως αποτέλεσμα της αναθεωρημένης οδηγίας NIS, από το 2022/23, ο ENISA θα διαθέτει πρόσθετους τομείς δράσης. Αν και αυτοί οι τομείς δράσης θα καλύπτονται από τα γενικά καθήκοντα του ENISA σύμφωνα με την εντολή του, θα έχουν ως αποτέλεσμα πρόσθετο φόρτο εργασίας για τον οργανισμό. Πιο συγκεκριμένα, εκτός από τους τρέχοντες τομείς δράσης του, βάσει της πρότασης της Επιτροπής για αναθεωρημένη οδηγία NIS, θα απαιτηθεί επίσης από τον ENISA να ενσωματώσει ειδικά στο πρόγραμμα εργασίας του, μεταξύ άλλων, τις ακόλουθες δράσεις: i) ανάπτυξη και τήρηση ευρωπαϊκού

[57] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης, καθώς και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον ιστότοπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EL/man/budgmanag/Pages/budgmanag.aspx.

μητρώου τρωτών σημείων (άρθρο 6 παράγραφος 2 της πρότασης), ii) παροχή γραμματειακής υποστήριξης στο ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (CyCLONe) (άρθρο 14 της πρότασης) και έκδοση ετήσιας έκθεσης σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ (άρθρο 15 της πρότασης), iii) υποστήριξη της διοργάνωσης αξιολογήσεων από ομοτίμους μεταξύ των κρατών μελών (άρθρο 16 της πρότασης), iv) συλλογή συγκεντρωτικών δεδομένων περιστατικών από τα κράτη μέλη και έκδοση τεχνικής καθοδήγησης (άρθρο 20 παράγραφος 9 της πρότασης), v) δημιουργία και τήρηση μητρώου για οντότητες που παρέχουν διασυνοριακές υπηρεσίες (άρθρο 25 της πρότασης).

Κατά συνέπεια, θα υποβληθεί αίτημα για 5 συμπληρωματικά ΙΠΑ από το 2022, καθώς και για τον αντίστοιχο προϋπολογισμό ύψους περίπου 0,61 εκατ. EUR ετησίως για την κάλυψη αυτών των νέων θέσεων.

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι.

Η Επιτροπή θα επανεξετάζει περιοδικά τη λειτουργία της οδηγίας και θα υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, την πρώτη φορά τρία έτη μετά την έναρξη ισχύος της.

Η Επιτροπή θα αξιολογήσει επίσης την ορθή μεταφορά της οδηγίας από τα κράτη μέλη.

Η παρακολούθηση και η υποβολή εκθέσεων σχετικά με την πρόταση θα συνάδουν με τις αρχές που περιγράφονται στη μόνιμη εντολή του ENISA δυνάμει του κανονισμού (ΕΕ) 2019/881 (πράξη για την κυβερνοασφάλεια).

Οι πηγές δεδομένων που θα χρησιμοποιούνται για την προγραμματιζόμενη παρακολούθηση θα προέρχονται κυρίως από τον ENISA, την ομάδα συνεργασίας, το δίκτυο CSIRT και τις αρχές των κρατών μελών. Εκτός από τα δεδομένα που συλλέγονται από τις εκθέσεις (συμπεριλαμβανομένων των ετήσιων εκθέσεων δραστηριοτήτων) του ENISA, την ομάδα συνεργασίας και το δίκτυο CSIRT, θα ήταν δυνατό να χρησιμοποιούνται, όταν χρειάζεται, ειδικά εργαλεία συλλογής δεδομένων (π.χ. έρευνες στις εθνικές αρχές, το Ευρωβαρόμετρο και εκθέσεις από την εκστρατεία του μήνα για την κυβερνοασφάλεια και από τις πανευρωπαϊκές ασκήσεις).

2.2. Συστήματα διαχείρισης και ελέγχου

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου

Η Διοικητική Μονάδα εντός της ΓΔ CNECT που είναι αρμόδια για τον τομέα πολιτικής θα διαχειρίζεται την εφαρμογή της οδηγίας.

Όσον αφορά τη διαχείριση του ENISA, στο άρθρο 15 της πράξης για την κυβερνοασφάλεια παρέχεται λεπτομερής κατάλογος των καθηκόντων ελέγχου του διοικητικού συμβουλίου του ENISA.

Σύμφωνα με το άρθρο 31 της πράξης για την κυβερνοασφάλεια, ο εκτελεστικός διευθυντής του ENISA είναι υπεύθυνος για την εκτέλεση του προϋπολογισμού του ENISA και ο εσωτερικός ελεγκτής της Επιτροπής ασκεί τις ίδιες εξουσίες έναντι του ENISA όπως και έναντι των υπηρεσιών της Επιτροπής. Το διοικητικό συμβούλιο του ENISA γνωμοδοτεί επί των οριστικών λογαριασμών του ENISA.

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους

Πολύ χαμηλός κίνδυνος, δεδομένου ότι το οικοσύστημα της οδηγίας NIS υφίσταται ήδη και καλύπτει ήδη τον ENISA, ο οποίος έχει μόνιμη εντολή μετά την έναρξη ισχύος της πράξης για την κυβερνοασφάλεια το 2019.

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)

Το αίτημα αύξησης του προϋπολογισμού αφορά την εφαρμογή του τίτλου 1 και προορίζεται για τη χρηματοδότηση μισθών. Αυτό σημαίνει πολύ χαμηλό κίνδυνο σφάλματος σε επίπεδο πληρωμών.

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.

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

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

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

- Δυνάμει του άρθρου 33 της πράξης για την κυβερνοασφάλεια, έως τις 28 Δεκεμβρίου 2019, ο ENISA προσχώρησε στη διοργανική συμφωνία της 25ης Μαΐου 1999 μεταξύ του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου της Ευρωπαϊκής Ένωσης και της Επιτροπής των Ευρωπαϊκών Κοινοτήτων σχετικά με τις εσωτερικές έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF). Ο ENISA εκδίδει αμελλητί τις ενδεδειγμένες διατάξεις που εφαρμόζονται σε όλους τους υπαλλήλους του οργανισμού.

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

- Υφιστάμενες γραμμές του προϋπολογισμού

Κατά σειρά τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ[58]	χωρών ΕΖΕΣ[59]	υποψηφίων για ένταξη χωρών[60]	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού
2	02 10 04	/ΜΔΠ	ΝΑΙ	ΟΧΙ	ΟΧΙ	/ΟΧΙ

[58] ΔΠ = Διαχωριζόμενες πιστώσεις / ΜΔΠ = Μη διαχωριζόμενες πιστώσεις.

[59] ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

[60] Υποψήφιες χώρες και, κατά περίπτωση, δυνάμει υποψήφια μέλη της ΕΕ από τα Δυτικά Βαλκάνια.

- Νέες γραμμές του προϋπολογισμού, των οποίων έχει ζητηθεί η δημιουργία

Κατά σειρά τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ	χωρών ΕΖΕΣ	υποψηφίων για ένταξη χωρών	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού
	[XX.YY.YY.YY]		ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ

3.2. Εκτιμώμενες επιπτώσεις στις δαπάνες

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις δαπάνες

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Αριθμός	[Τομέας... 2 Ενιαία αγορά, καινοτομία και ψηφιακή οικονομία.....]

[Φορέας]: <…ENISA….>			Έτος **N**[61] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) **2026**	**2027**		**ΣΥΝΟΛΟ**
Τίτλος 1:	Αναλήψεις υποχρεώσεων	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Πληρωμές	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Τίτλος 2:	Αναλήψεις υποχρεώσεων	(1α)								
	Πληρωμές	(2α)								
Τίτλος 3:	Αναλήψεις υποχρεώσεων	(3α)								
	Πληρωμές	(3β)								
ΣΥΝΟΛΟ πιστώσεων για τον [οργανισμό] <ENISA…….>	Αναλήψεις υποχρεώσεων	=1+1α +3α	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Πληρωμές	=2+2α +3β	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] Το έτος N είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «N» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

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

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)			**ΣΥΝΟΛΟ**
ΓΔ: <…….>									
• Ανθρώπινοι πόροι									
• Άλλες διοικητικές δαπάνες									
ΣΥΝΟΛΟ ΓΔ <…….>	Πιστώσεις								

ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 5 του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών)								

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		Έτος **N**[62] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) **2026**	**2027**		**ΣΥΝΟΛΟ**
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 5 του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Πληρωμές	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] Το έτος N είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «N» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

3.2.2. Εκτιμώμενες επιπτώσεις στις πιστώσεις [του οργανισμού]

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

– ☐ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω.

Πιστώσεις αναλήψεων υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			Έτος **N**		Έτος **N+1**		Έτος **N+2**		Έτος **N+3**		Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)						**ΣΥΝΟΛΟ**	
	ΑΠΟΤΕΛΕΣΜΑΤΑ																	
	Είδος[63]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[64] …																		
- Αποτέλεσμα																		
- Αποτέλεσμα																		
- Αποτέλεσμα																		
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1																		
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ...																		
- Αποτέλεσμα																		
Μερικό σύνολο για τον ειδικό στόχο αριθ. 2																		

[63] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[64] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ															

3.2.3. Εκτιμώμενες επιπτώσεις στο ανθρώπινο δυναμικό του ENISA

3.2.3.1. Συνοπτική παρουσίαση

Ως αποτέλεσμα της αναθεωρημένης οδηγίας NIS, από το 2022/23, ο ENISA θα έχει πρόσθετα καθήκοντα. Αν και αυτά τα καθήκοντα θα καλύπτονται από την εντολή του ENISA, θα έχουν ως αποτέλεσμα πρόσθετο φόρτο εργασίας για τον οργανισμό. Πιο συγκεκριμένα, εκτός από τα τρέχοντα καθήκοντά του, βάσει της πρότασης της Επιτροπής για αναθεωρημένη οδηγία NIS, ο ENISA θα επιφορτισθεί, μεταξύ άλλων, με i) την ανάπτυξη και τήρηση ευρωπαϊκού μητρώου τρωτών σημείων (άρθρο 6 παράγραφος 2), ii) την παροχή γραμματειακής υποστήριξης στο ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (CyCLONe) (άρθρο 14) και την έκδοση ετήσιας έκθεσης σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ (άρθρο 15), iii) την υποστήριξη της διοργάνωσης αξιολογήσεων από ομοτίμους μεταξύ των κρατών μελών (άρθρο 16), iv) τη συλλογή συγκεντρωτικών δεδομένων περιστατικών από τα κράτη μέλη και έκδοση τεχνικής καθοδήγησης (άρθρο 20 παράγραφος 9), v) τη δημιουργία και τήρηση μητρώου για οντότητες που παρέχουν διασυνοριακές υπηρεσίες (άρθρο 25).

Κατά συνέπεια, θα υποβληθεί αίτημα για 5 συμπληρωματικά ΙΠΑ από το 2022, καθώς και για τον αντίστοιχο προϋπολογισμό για την κάλυψη αυτών των νέων θέσεων.

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

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

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

	Έτος **N** [65] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) **2026** **2027**			**ΣΥΝΟΛΟ**
Έκτακτοι υπάλληλοι (βαθμοί AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Έκτακτοι υπάλληλοι (βαθμοί AST)								
Συμβασιούχοι υπάλληλοι	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Αποσπασμένοι εθνικοί εμπειρογνώμονες								

[65] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «Ν» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

ΣΥΝΟΛΟ	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Απαιτήσεις προσωπικού (ΙΠΑ):

	Έτος **N** [66] **2022**	Έτος **N+1** **2023**	Έτος **N+2** **2024**	Έτος **N+3** **2025**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6) **2026** **2027**			**ΣΥΝΟΛΟ**
Έκτακτοι υπάλληλοι (βαθμοί AD)	3	3	3	3	3	3		**18**
Έκτακτοι υπάλληλοι (βαθμοί AST)								
Συμβασιούχοι υπάλληλοι	2	2	2	2	2	2		**12**
Αποσπασμένοι εθνικοί εμπειρογνώμονες								

ΣΥΝΟΛΟ	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους για την αρμόδια ΓΔ

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

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

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

	Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)		
• **Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)**							
XX 01 01 01 (στην έδρα και στις αντιπροσωπείες της Επιτροπής)							
XX 01 01 02 (στις αντιπροσωπείες της ΕΕ)							

66 Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «Ν» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

XX 01 05 01 (έμμεση έρευνα)								
10 01 05 01 (άμεση έρευνα)								
• Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)[67]								
XX 01 02 01 (AC, END, INT από το συνολικό κονδύλιο)								
XX 01 02 02 (AC, AL, END, INT και JPD στις αντιπροσωπείες της ΕΕ)								
XX 01 04 ***yy***[68]	- στην έδρα[69]							
	- στις αντιπροσωπείες της ΕΕ							
XX 01 05 02 (AC, END, INT – έμμεση έρευνα)								
10 01 05 02 (AC, END, INT – άμεση έρευνα)								
Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν)								
ΣΥΝΟΛΟ								

XX είναι ο σχετικός τομέας πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού.

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	
Εξωτερικό προσωπικό	

Η περιγραφή του υπολογισμού του κόστους των θέσεων που εκφράζονται σε μονάδες πλήρους απασχόλησης θα πρέπει να περιλαμβάνεται στο τμήμα 3 του παραρτήματος V.

67 AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

68 Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

69 Κυρίως για τα διαρθρωτικά ταμεία, το Ευρωπαϊκό Γεωργικό Ταμείο Αγροτικής Ανάπτυξης (ΕΓΤΑΑ) και το Ευρωπαϊκό Ταμείο Αλιείας (ΕΤΑ).

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

– ☒ Η πρόταση/πρωτοβουλία είναι συμβατή με το ισχύον πολυετές δημοσιονομικό πλαίσιο.

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

Να εξηγηθεί ο απαιτούμενος αναπρογραμματισμός και να προσδιοριστούν οι σχετικές γραμμές του προϋπολογισμού και τα αντίστοιχα ποσά. Η πρόταση είναι συμβατή με το ΠΔΠ 21/27. Η αντιστάθμιση του προϋπολογισμού που ζητείται για να καλυφθεί η αύξηση των ανθρώπινων πόρων στον ENISA θα επιτευχθεί με τη μείωση του προϋπολογισμού του προγράμματος «Ψηφιακή Ευρώπη» (DEP) στον ίδιο τομέα, κατά το ίδιο ποσό.

– ☐ Η πρόταση/πρωτοβουλία απαιτεί τη χρησιμοποίηση του μηχανισμού ευελιξίας ή την αναθεώρηση του πολυετούς δημοσιονομικού πλαισίου[70].

Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, καθώς και τα αντίστοιχα ποσά.

3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση

– Η πρόταση/πρωτοβουλία δεν προβλέπει συγχρηματοδότηση από τρίτους.

– Η πρόταση/πρωτοβουλία προβλέπει τη συγχρηματοδότηση που εκτιμάται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

	Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)			Σύνολο
Προσδιορισμός του φορέα συγχρηματοδότησης								
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων								

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

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

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

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

☐ στους ιδίους πόρους

☐ στα λοιπά έσοδα

☐ Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Γραμμή εσόδων του προϋπολογισμού:	Διαθέσιμες πιστώσεις για το τρέχον οικονομικό έτος	Επιπτώσεις της πρότασης/πρωτοβουλίας[71]						
		Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)		
Άρθρο …….								

Ως προς τα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

Να προσδιοριστεί η μέθοδος υπολογισμού των επιπτώσεων στα έσοδα.

[71] Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.