ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Πρόταση

ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση

{SWD(2013) 31 final}
{SWD(2013) 32 final}

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

Σκοπός της προτεινόμενης οδηγίας είναι να εξασφαλιστεί κοινό υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών (NIS/ΑΔΠ). Αυτό σημαίνει βελτίωση της ασφάλειας του διαδικτύου και των ιδιωτικών δικτύων και συστημάτων πληροφοριών που υποστηρίζουν τη λειτουργία των κοινωνιών και των οικονομιών μας. Τα παραπάνω θα επιτευχθούν απαιτώντας από τα κράτη μέλη να αυξήσουν την ετοιμότητά τους, να βελτιώσουν τη μεταξύ τους συνεργασία, και ζητώντας από τους φορείς εκμετάλλευσης των υποδομών ζωτικής σημασίας, όπως είναι η ενέργεια, οι μεταφορές, καθώς και από τους βασικούς παρόχους υπηρεσιών της κοινωνίας της πληροφορίας (πλατφόρμες ηλ-εμπορίου, κοινωνικά δίκτυα , κλπ), όπως και από τις δημόσιες διοικήσεις να θεσπίσουν κατάλληλα μέτρα για τη διαχείριση των κινδύνων για την ασφάλεια και να αναφέρουν τα σοβαρά συμβάντα στις αρμόδιες εθνικές αρχές.

Η παρούσα πρόταση υποβάλλεται σε συνδυασμό με την κοινή ανακοίνωση της Επιτροπής και της Ύπατης Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφάλειας για μια ευρωπαϊκή στρατηγική ασφάλειας του κυβερνοχώρου. Ο στόχος της στρατηγικής είναι να διασφαλιστεί ασφαλές και αξιόπιστο ψηφιακό περιβάλλον, με παράλληλη προώθηση και προστασία των θεμελιωδών δικαιωμάτων και λοιπών θεμελιωδών αξιών της ΕΕ. Η παρούσα πρόταση αποτελεί την κύρια δράση της στρατηγικής. Περαιτέρω δράσεις στα πλαίσια αυτής της στρατηγικής στο πεδίο αυτό επικεντρώνονται στην αύξηση της ευαισθητοποίησης, στην ανάπτυξη εσωτερικής αγοράς για προϊόντα και υπηρεσίες της ασφάλειας στον κυβερνοχώρο, καθώς και στην προώθηση των επενδύσεων σε Ε&Α. Οι δράσεις αυτές θα πλαισιωθούν από άλλες, με σκοπό να επιταχυνθεί η καταπολέμηση του ηλεκτρονικού εγκλήματος και να συγκροτηθεί διεθνής πολιτική για την ασφάλεια του κυβερνοχώρου, σε ενωσιακή κλίμακα.

1.1. Αιτιολόγηση και στόχοι της πρότασης

Η ΑΔΠ αποκτά διαρκώς μεγαλύτερη σημασία για την οικονομία και την κοινωνία μας. Η ΑΔΠ είναι επίσης απαραίτητη προϋπόθεση ώστε να προκύψει αξιόπιστο περιβάλλον για το εμπόριο υπηρεσιών σε παγκόσμια κλίμακα. Ωστόσο, τα συστήματα πληροφοριών μπορεί να πληγούν από συμβάντα που θέτουν σε κίνδυνο την ασφάλεια, όπως είναι τα ανθρώπινα λάθη, φυσικά φαινόμενα, τεχνικές αστοχίες ή κακόβουλες επιθέσεις. Τα συμβάντα αυτά καθίστανται μεγαλύτερα, πιο σύνθετα, και εμφανίζονται με μεγαλύτερη συχνότητα. Από τη διαδικτυακή δημόσια διαβούλευση της Επιτροπής σχετικά με τη «βελτίωση της ασφάλειας δικτύων και πληροφοριών στην ΕΕ»[1] προκύπτει ότι**,** κατά το προηγούμενο έτος, ποσοστό 57% των ερωτηθέντων είχε εμπειρία συμβάντων ΑΔΠ με σοβαρές επιπτώσεις στις δραστηριότητές τους. Η απουσία ΑΔΠ μπορεί να θέσει σε κίνδυνο ζωτικές υπηρεσίες που εξαρτώνται από την ακεραιότητα των συστημάτων δικτύων και πληροφοριών. Αυτό μπορεί να οδηγήσει στη διακοπή της λειτουργίας επιχειρήσεων, να προκαλέσει σημαντικές οικονομικές ζημίες για την οικονομία της ΕΕ και να επηρεάσει δυσμενώς την κοινωνική ευημερία.

Επιπλέον, ως μέσο επικοινωνίας χωρίς σύνορα, τα ψηφιακά συστήματα πληροφοριών, ιδίως το διαδίκτυο, είναι διασυνδεμένα μεταξύ των κρατών μελών και διαδραματίζουν ουσιαστικό ρόλο στην προώθηση της διασυνοριακής κυκλοφορίας των εμπορευμάτων, των υπηρεσιών και των προσώπων. Σημαντική διαταραχή των συστημάτων αυτών σε ένα κράτος μέλος μπορεί να πλήξει άλλα κράτη μέλη και την ΕΕ στο σύνολό της. Η ανθεκτικότητα και η σταθερότητα των συστημάτων δικτύων και πληροφοριών είναι επομένως απαραίτητη για την ολοκλήρωση της ψηφιακής ενιαίας αγοράς και για την ομαλή λειτουργία της εσωτερικής

[1] Η διαδικτυακή δημόσια διαβούλευση με θέμα «βελτίωση της ασφάλειας δικτύων και πληροφοριών στην ΕΕ», διεξήχθη από τις 23 Ιουλίου έως τις 15 Οκτωβρίου 2012.

αγοράς. Η πιθανότητα και η συχνότητα των συμβάντων και η αδυναμία διασφάλισης αποτελεσματικής προστασίας επίσης υπονομεύουν την πίστη και εμπιστοσύνη του κοινού σε υπηρεσίες δικτύων και πληροφοριών: για παράδειγμα, το Ευρωβαρόμετρο του 2012 με αντικείμενο την ασφάλεια στον κυβερνοχώρο διαπιστώνει ότι το 38% των χρηστών του διαδικτύου στην ΕΕ ανησυχεί για την ασφάλεια των ηλεκτρονικών πληρωμών και ότι έχουν αλλάξει συμπεριφορά λόγω της ανησυχίας που τους εμπνέει το ζήτημα της ασφάλειας: το 18% είναι μάλλον απίθανο να αγοράσει προϊόντα στο διαδίκτυο, ενώ το 15% είναι μάλλον απίθανο να κάνει χρήση επιγραμμικών (διαδικτυακών) τραπεζικών υπηρεσιών[2].

Η σημερινή κατάσταση στην ΕΕ, αντικατοπτρίζοντας την καθαρά εθελοντική προσέγγιση που έχει ακολουθηθεί μέχρι σήμερα, δεν παρέχει επαρκή προστασία έναντι συμβάντων και κινδύνων ΑΔΠ σε ολόκληρη την ΕΕ. Οι υφιστάμενες ικανότητες και μηχανισμοί ΑΔΠ είναι σαφώς ανεπαρκείς ώστε να συμβαδίσουν με την ταχέως μεταβαλλόμενη μορφολογία των απειλών και να εξασφαλίσουν κοινό υψηλό επίπεδο προστασίας σε όλα τα κράτη μέλη.

Παρά τις πρωτοβουλίες που έχουν αναληφθεί, τα κράτη μέλη έχουν πολύ διαφορετικά επίπεδα ικανοτήτων και ετοιμότητας, με αποτέλεσμα κατακερματισμένες προσεγγίσεις σε ολόκληρη την ΕΕ. Δεδομένου ότι δίκτυα και συστήματα είναι διασυνδεδεμένα, η συνολική ασφάλεια δικτύων και υπηρεσιών αποδυναμώνεται από τα κράτη μέλη με ανεπαρκές επίπεδο προστασίας. Η κατάσταση αυτή παρεμποδίζει επίσης την οικοδόμηση εμπιστοσύνης μεταξύ ομοτίμων, η οποία αποτελεί προϋπόθεση για τη συνεργασία και την ανταλλαγή πληροφοριών. Ως αποτέλεσμα, συνεργασία υπάρχει μόνο σε μια μειονότητα κρατών μελών που διαθέτουν υψηλό επίπεδο ικανοτήτων.

Επομένως, δεν υφίσταται προς το παρόν σε ενωσιακό επίπεδο αποτελεσματικός μηχανισμός μεταξύ των κρατών μελών για ουσιαστική συνεργασία και ασφαλή ανταλλαγή πληροφοριώσε ν σχετικά με συμβάντα ΑΔΠ και συναφείς κινδύνους. Αυτό μπορεί να οδηγήσει σε ασυντόνιστες ρυθμιστικές παρεμβάσεις, σε μη συνεκτικές στρατηγικές και σε αποκλίνοντα πρότυπα, με αποτέλεσμα ανεπαρκή προστασία όσον αφορά την ΑΔΠ σε ολόκληρη την ΕΕ. Μπορεί επίσης να προκύψουν εμπόδια στην εσωτερική αγορά, προκαλώντας κόστος συμμόρφωσης για τις επιχειρήσεις που αναπτύσσουν δραστηριότητες σε περισσότερα από ένα κράτη μέλη.

Τέλος, οι φορείς που διαχειρίζονται υποδομές ζωτικής σημασίας ή παρέχουν υπηρεσίες απαραίτητες για τη λειτουργία των κοινωνιών μας δεν υπόκεινται σε υποχρεώσεις για θέσπιση μέτρων διαχείρισης του κινδύνου και ανταλλαγής πληροφοριών με τις αρμόδιες αρχές. Ως εκ τούτου, οι επιχειρήσεις αφενός στερούνται αποτελεσματικών κινήτρων για να ασκήσουν ενδελεχή διαχείριση κινδύνων, συμπεριλαμβανόμενης της αξιολόγησης κινδύνου και της λήψης ενδεδειγμένων μέτρων για να εξασφαλίσουν την ασφάλεια δικτύων και πληροφοριών (NIS). Αφετέρου, μεγάλο ποσοστό συμβάντων δεν καταλήγει στις αρμόδιες αρχές και περνά απαρατήρητο. Ωστόσο, η πληροφόρηση για τα συμβάντα είναι απαραίτητη ώστε οι δημόσιες αρχές να αντιδράσουν, να λάβουν κατάλληλα μέτρα περιστολής των κινδύνων και να καθορίσουν ενδεδειγμένες στρατηγικές προτεραιότητες όσον αφορά την NIS.

Το ισχύον κανονιστικό πλαίσιο απλώς απαιτεί από τις εταιρείες τηλεπικοινωνιών να θεσπίζουν μέτρα διαχείρισης του κινδύνου και να αναφέρουν τα σοβαρά συμβάντα ΑΔΠ. Ωστόσο, πολλοί άλλοι τομείς βασίζονται στις ΤΠΕ αποδίδοντάς τους ιδιότητες καταλύτη και ως εκ τούτου πρέπει εξίσου να ενδιαφέρονται για την ασφάλεια δικτύων και πληροφοριών. Μια σειρά από ειδικές υποδομές και παρόχους υπηρεσιών παρουσιάζουν ιδιαίτερα ευάλωτο χαρακτήρα, εξαιτίας της μεγάλης τους εξάρτησης από εύρυθμα λειτουργούντα συστήματα δικτύων και πληροφοριών. Οι εν λόγω τομείς διαδραματίζουν ουσιαστικό ρόλο στην παροχή

[2] Ευρωβαρόμετρο (390/2012)

βασικών υπηρεσιών υποστήριξης για την οικονομία και την κοινωνία μας, ενώ η ασφάλεια των συστημάτων τους έχει ιδιαίτερη σημασία για τη λειτουργία της εσωτερικής αγοράς. Οι τομείς αυτοί περιλαμβάνουν τις τράπεζες, τα χρηματιστήρια, την παραγωγή, μετάδοση και διανομή ενέργειας, τις μεταφορές (εναέριες, σιδηροδρομικές, θαλάσσιες), την υγεία, τις υπηρεσίες διαδικτύου και τη δημόσια διοίκηση.

Απαιτείται συνεπώς ριζική αλλαγή στον τρόπο με τον οποίο αντιμετωπίζεται η ΑΔΠ στην ΕΕ. Απαιτείται θέσπιση ρυθμιστικών υποχρεώσεων ώστε να προκύψουν ίσοι όροι ανταγωνισμού και να καλυφθούν υφιστάμενα νομοθετικά κενά. Για την αντιμετώπιση αυτών των προβλημάτων και για την αύξηση του επιπέδου της ασφάλειας δικτύων και πληροφοριών εντός της Ευρωπαϊκής Ένωσης, οι στόχοι της προτεινόμενης οδηγίας είναι οι εξής.

Πρώτον, η πρόταση απαιτεί από όλα τα κράτη μέλη να εξασφαλίσουν ότι έχει τεθεί σε εφαρμογή ένα ελάχιστο επίπεδο εθνικών ικανοτήτων, με τον καθορισμό αρχών αρμόδιων για την NIS, τη σύσταση ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και με τη θέσπιση εθνικών στρατηγικών ΑΔΠ και εθνικών σχεδίων συνεργασίας για την ασφάλεια δικτύων και πληροφοριών.

Δεύτερον, οι αρμόδιες εθνικές αρχές πρέπει να συνεργάζονται σε ένα δίκτυο που θα εξασφαλίζει ασφαλή και αποτελεσματικό συντονισμό, συμπεριλαμβανομένης της συντονισμένης ανταλλαγής πληροφοριών, καθώς και ανίχνευση και απόκριση σε επίπεδο ΕΕ. Μέσω του δικτύου αυτού, τα κράτη μέλη αναμένεται ότι θα ανταλλάσσουν πληροφορίες και θα συνεργάζονται για την αντιμετώπιση απειλών και συμβάντων σε βάρος της ΑΔΠ, με βάση το ευρωπαϊκό σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών.

Τρίτον, με βάση το υπόδειγμα της οδηγίας πλαίσιο για τις ηλεκτρονικές επικοινωνίες, η πρόταση αποσκοπεί να εξασφαλίσει την ανάπτυξη κλίματος διαχείρισης κινδύνων και την ανταλλαγή πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα. Οι εταιρείες στους συγκεκριμένους ζωτικούς τομείς που περιγράφονται παραπάνω και η δημόσια διοίκηση θα υποχρεούνται να εκτιμήσουν τους κινδύνους που αντιμετωπίζουν και να θεσπίζουν κατάλληλα και αναλογικά μέτρα προς εξασφάλιση της ασφάλειας δικτύων και πληροφοριών. Οι φορείς αυτοί θα οφείλουν να υποβάλλουν στις αρμόδιες αρχές οποιοδήποτε συμβάν ενδέχεται να θέσει σοβαρά σε κίνδυνο τα οικεία δίκτυα και συστήματα πληροφοριών και να επηρεάσει σημαντικά τη συνέχιση της παροχής των ζωτικής σημασίας υπηρεσιών και την παράδοση προϊόντων.

1.2. Γενικό πλαίσιο

Ήδη το 2001, στην ανακοίνωσή της για την ασφάλεια δικτύων και πληροφοριών: «Πρόταση ευρωπαϊκής πολιτικής», η Επιτροπή υπογράμμισε την αυξανόμενη σημασία της ΑΔΠ (ασφάλειας δικτύων και πληροφοριών)[3]. Ακολούθησε η έκδοση, το 2006, μιας στρατηγικής για ασφαλή κοινωνία της πληροφορίας[4], με στόχο την ανάπτυξη κλίματος συνεργασίας για την ασφάλεια δικτύων και πληροφοριών στην Ευρώπη. Τα κυριότερα στοιχεία της εγκρίθηκαν σε ψήφισμα του Συμβουλίου[5].

Επίσης, στις 30 Μαρτίου 2009, η Επιτροπή εξέδωσε ανακοίνωση σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας (CIIP)[6] με επίκεντρο την προστασία της Ευρώπης από διαταραχές στον κυβερνοχώρο μέσω ενίσχυσης της ασφάλειας. Η Επιτροπή δρομολόγησε σχέδιο δράσης σε υποστήριξη των προσπαθειών των κρατών μελών να εξασφαλίσουν πρόληψη και αντίδραση. Το σχέδιο δράσης εγκρίθηκε στα συμπεράσματα της

---

3 COM (2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf
5 2007/068/01.
6 COM (2009) 149.

προεδρίας της υπουργικής διάσκεψης για τις CIIP στο Τάλιν το 2009. Στις 18 Δεκεμβρίου 2009, το Συμβούλιο εξέδωσε ψήφισμα με θέμα «μια ευρωπαϊκή συνεργατική προσέγγιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών»[7].

Στο ψηφιακό θεματολόγιο για την Ευρώπη[8], το οποίο εγκρίθηκε τον Μάιο του 2010, και στα σχετικά συμπεράσματα του Συμβουλίου[9] τονίζεται η κοινή πεποίθηση ότι η εμπιστοσύνη και η ασφάλεια αποτελούν θεμελιώδεις προϋποθέσεις για την ευρεία αφομοίωση των ΤΠΕ και, ως εκ τούτου, για την επίτευξη των στόχων της διάστασης της στρατηγικής «Ευρώπη 2020» που αφορά την «έξυπνη ανάπτυξη»[10]. Στο κεφάλαιο εμπιστοσύνη και ασφάλεια, το Ψηφιακό θεματολόγιο υπογραμμίζει την ανάγκη όλοι οι ενδιαφερόμενοι να ενώσουν τις δυνάμεις σε μιαν ενιαία προσπάθεια προκειμένου να εξασφαλιστεί η ασφάλεια και η ανθεκτικότητα της υποδομής σε ΤΠΕ, δίνοντας έμφαση στην πρόληψη, την ετοιμότητα και την ευαισθητοποίηση του κοινού, καθώς και για την ανάπτυξη αποτελεσματικών και συντονισμένων μηχανισμών ασφαλείας. Ειδικότερα, η κεντρική δράση 6 του Ψηφιακού θεματολογίου για την Ευρώπη απαιτεί μέτρα που αποβλέπουν σε ενισχυμένη και υψηλού επιπέδου πολιτική ασφάλειας δικτύων και πληροφοριών.

Στην ανακοίνωσή της για τις CIIP τον Μάρτιο του 2011, με τίτλο «Επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο»[11], η Επιτροπή έκανε τον απολογισμό των αποτελεσμάτων που επιτεύχθηκαν μετά την έγκριση του σχεδίου δράσης CIIP το 2009, καταλήγοντας στο συμπέρασμα ότι από την εφαρμογή του προγράμματος προέκυψε ότι οι αμιγώς εθνικές προσεγγίσεις για την αντιμετώπιση των προκλήσεων που αφορούν την ασφάλεια και την ανθεκτικότητα δεν επαρκούν, και ότι η Ευρώπη πρέπει να συνεχίσει τις προσπάθειες για την οικοδόμηση μιας συνεκτικής και συνεργατικής προσέγγισης σε ολόκληρη την ΕΕ. Στην ανακοίνωση του 2011 για τις CIIP αναγγέλθηκε σειρά δράσεων, ενώ η Επιτροπή καλεί τα κράτη μέλη να συγκροτήσουν ικανότητες ΑΔΠ και διασυνοριακή συνεργασία. Οι περισσότερες από τις δράσεις αυτές πρέπει να έχουν ολοκληρωθεί το 2012, αλλά δεν έχουν ακόμα υλοποιηθεί.

Στα συμπεράσματά του της 27ης Μαΐου 2011 για τις CIIP, το Ευρωπαϊκό Συμβούλιο υπογράμμισε την επείγουσα ανάγκη τα συστήματα και τα δίκτυα ΤΠΕ να καταστούν ανθεκτικά και ασφαλή από κάθε πιθανή διαταραχή, τυχαία ή εσκεμμένη, να αναπτυχθεί σε ολόκληρη την ΕΕ υψηλό επίπεδο ετοιμότητας, ασφάλειας και ανθεκτικότητας των ικανοτήτων, να αναβαθμιστούν οι τεχνικές ικανότητες ώστε να μπορέσει η Ευρώπη να αντιμετωπίσει τα προβλήματα που συνεπάγεται η προστασία δικτύων και υποδομών πληροφοριών, καθώς και να ενισχυθεί η συνεργασία μεταξύ των κρατών μελών με την ανάπτυξη μηχανισμών συνεργασίας μεταξύ των κρατών μελών έναντι συμβάντων ασφάλειας.

1.3. Ισχύουσες διατάξεις της Ευρωπαϊκής Ένωσης και διεθνείς διατάξεις στον συγκεκριμένο τομέα

Δυνάμει του κανονισμού (ΕΚ) αριθ. 460/2004, η Ευρωπαϊκή Κοινότητα ίδρυσε, το 2004, τον Ευρωπαϊκό Οργανισμό Ασφάλειας Δικτύων και Πληροφοριών (ENISA)[12], με σκοπό να συμβάλει στο να εξασφαλιστεί υψηλό επίπεδο και να αναπτυχθεί στην ΕΕ κλίμα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών. Στις 30 Σεπτεμβρίου 2010 εγκρίθηκε πρόταση

---

7 2009/C 321/01.

8 COM (2010) 245.

9 Συμπεράσματα του Συμβουλίου της 31ης Μαΐου 2010 σχετικά με το Ψηφιακό θεματολόγιο για την Ευρώπη (10130/10)

10 COM(2010) 2020 και συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 25/26 Μαρτίου 2010 (EUCO 7/10).

11 COM (2011) 163.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EL:HTML

για τον εκσυγχρονισμό της εντολής του ENISA[13], η οποία εξετάζεται στο Συμβούλιο και στο Ευρωπαϊκό Κοινοβούλιο. Το αναθεωρημένο κανονιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες[14], το οποίο ισχύει από τον Νοέμβριο του 2009, επιβάλλει υποχρεώσεις ασφάλειας στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών[15]. Οι υποχρεώσεις αυτές έπρεπε τον Μάιο του 2011 να είχαν μεταφερθεί στο εθνικό δίκαιο.

Όλοι οι συντελεστές οι οποίοι είναι υπεύθυνοι επεξεργασίας δεδομένων (π.χ. τράπεζες ή νοσοκομεία) υποχρεούνται, βάσει του κανονιστικού πλαισίου για την προστασία των δεδομένων[16], να θεσπίσουν μέτρα ασφάλειας για την προστασία των δεδομένων προσωπικού χαρακτήρα. Επίσης, βάσει της πρότασης του 2012 της Επιτροπής για γενικό κανονισμό για την προστασία των δεδομένων[17], οι υπεύθυνοι επεξεργασίας δεδομένων θα υποχρεούνται να κοινοποιούν στις εθνικές εποπτικές αρχές τις παραβιάσεις προσωπικών δεδομένων. Αυτό σημαίνει ότι, για παράδειγμα, μια παραβίαση ασφάλειας ΑΔΠ που επηρεάζει την παροχή μιας υπηρεσίας χωρίς να συντρέχει διακύβευση προσωπικών δεδομένων (π.χ. διακοπής λειτουργίας ΤΠΕ σε μια εταιρεία ηλεκτρισμού με αποτέλεσμα τη διακοπή ρεύματος) δεν θα απαιτείται να κοινοποιείται.

Σύμφωνα με την οδηγία 2008/114 σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την αξιολόγηση της ανάγκης για βελτίωση της προστασίας τους, το «Ευρωπαϊκό πρόγραμμα για την προστασία των υποδομών ζωτικής σημασίας (EPCIP)»[18] καθορίζει το υποκείμενο πλαίσιο προσέγγισης για την προστασία των υποδομών ζωτικής σημασίας στην ΕΕ. Οι στόχοι του EPCIP (Ευρωπαϊκό πρόγραμμα προστασίας των υποδομών ζωτικής σημασίας) συνάδουν πλήρως με την παρούσα πρόταση και η οδηγία αναμένεται να ισχύσει με την επιφύλαξη της οδηγίας 2008/114. Το EPCIP δεν υποχρεώνει τους φορείς εκμετάλλευσης να αναφέρουν σημαντικές παραβιάσεις της ασφάλειας και δεν θεσπίζει μηχανισμούς ώστε τα κράτη μέλη να συνεργάζονται και να αντιδρούν σε περίπτωση συμβάντων.

Οι συννομοθέτες εξετάζουν την πρόταση της Επιτροπής για θέσπιση οδηγίας σχετικά με επιθέσεις κατά συστημάτων πληροφοριών[19], η οποία έχει ως στόχο να εναρμονίσει την ποινικοποίηση συγκεκριμένων τύπων συμπεριφοράς. Καλύπτει μόνον την ποινικοποίηση συγκεκριμένων τύπων συμπεριφοράς και δεν εξετάζει την πρόληψη κινδύνων και συμβάντων NIS, την αντιμετώπιση συμβάντων ΑΔΠ και τον μετριασμό των επιπτώσεών τους. Η παρούσα οδηγία πρέπει να εφαρμόζεται με την επιφύλαξη της οδηγίας για τις επιθέσεις κατά των συστημάτων πληροφοριών.

Στις 28 Μαρτίου 2012, η Επιτροπή εξέδωσε ανακοίνωση για τη δημιουργία Ευρωπαϊκού Κέντρου για εγκλήματα στον κυβερνοχώρο(EC3)[20]. Το κέντρο αυτό, που ιδρύθηκε στις 11 Ιανουαρίου 2013, είναι μέρος της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Ευρωπόλ) και θα λειτουργεί ως εστιακό σημείο για την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο στην ΕΕ. Το EC3 προορίζεται να συγκεντρώνει την ευρωπαϊκή εμπειρογνωμοσύνη στο πεδίο του εγκλήματος στον κυβερνοχώρο προκειμένου να ενισχυθούν τα κράτη μέλη στην ανάπτυξη ικανοτήτων, να στηρίζει τις έρευνες των κρατών μελών για τα

---

13 COM (2010) 521.

14 Βλ. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Άρθρα 13α και 13β της οδηγίας πλαίσιο.

16 Οδηγία 2002/58 της 12ης Ιουλίου 2002

17 COM (2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

19 COM(2010)517 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EL:PDF

20 COM(2012)140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EL:PDF

εγκλήματα στον κυβερνοχώρο και, σε στενή συνεργασία με την Eurojust, να καταστεί η συλλογική φωνή των ευρωπαίων φορέων διερεύνησης εγκλημάτων στον κυβερνοχώρο, στην επιβολή του νόμου και στη δικαιοσύνη.

Τα ευρωπαϊκά θεσμικά όργανα, οι οργανισμοί και οι υπηρεσίες της ΕΕ έχουν ιδρύσει ιδιαίτερη ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική, με την επωνυμία CERT-EU.

Σε διεθνές επίπεδο, η ΕΕ συνεργάζεται με αντικείμενο την ασφάλεια στον κυβερνοχώρο, τόσο σε διμερές, όσο και σε πολυμερές επίπεδο. Κατά τη διάσκεψη κορυφής ΕΕ-ΗΠΑ του 2010[21] ιδρύθηκε η ομάδα εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στον κυβερνοχώρο και το ηλεκτρονικό έγκλημα. Η ΕΕ δραστηριοποιείται επίσης σε άλλα συναφή πολυμερή φόρουμ, όπως ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ), η Γενική Συνέλευση του ΟΗΕ (ΓΣ ΗΕ), η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ), η Παγκόσμια Διάσκεψη Κορυφής για την Πληροφοριών Κοινωνία (WSIS) και το Φόρουμ για τη Διακυβέρνηση του Διαδικτύου (IGF).

2. ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΔΙΑΒΟΥΛΕΥΣΕΩΝ ΜΕ ΤΑ ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ ΚΑΙ ΕΚΤΙΜΗΣΕΙΣ ΤΟΥ ΑΝΤΙΚΤΥΠΟΥ

2.1. Διαβουλεύσεις με ενδιαφερόμενα μέρη και χρήση εμπειρογνωμοσύνης

Μεταξύ 23 Ιουλίου και 15 Οκτωβρίου 2012 πραγματοποιήθηκε δημόσια διαβούλευση μέσω διαδικτύου σχετικά με «τη βελτίωση της ασφάλειας δικτύων και πληροφοριών στην ΕΕ». Συνολικά, η Επιτροπή παρέλαβε 160 απαντήσεις στο διαδικτυακό ερωτηματολόγιο.

Το βασικό αποτέλεσμα ήταν ότι οι ενδιαφερόμενοι φορείς υποστήριξαν εν γένει την ανάγκη βελτίωσης της ασφάλειας δικτύων και πληροφοριών (NIS) σε όλη την ΕΕ. Πιο συγκεκριμένα: Ποσοστό 82,8% των ερωτηθέντων εξέφρασε την άποψη ότι οι κυβερνήσεις της ΕΕ πρέπει να πράξουν περισσότερα για να εξασφαλιστεί υψηλό επίπεδο ΑΔΠ το 82,8 % ήταν της γνώμης ότι οι χρήστες πληροφοριών και συστημάτων δεν γνωρίζουν τις υφιστάμενες απειλές για την ΑΔΠ και τα σχετικά συμβάντα · το 66,3% θα ήταν, κατ' αρχήν, υπέρ της θέσπισης κανονιστικής απαίτησης για τη διαχείριση κινδύνων για την NIS· και το 84,8% δήλωσε ότι οι απαιτήσεις αυτές πρέπει να καθοριστούν σε επίπεδο ΕΕ. Μεγάλος αριθμός ερωτηθέντων θεωρεί ότι θα ήταν σημαντικό να θεσπιστούν απαιτήσεις ΑΔΠ στους ακόλουθους τομείς: τραπεζικές και χρηματοπιστωτικές υπηρεσίες (91,1%), ενέργεια (89,4%), μεταφορές (81,7%), υγεία (89,4%), υπηρεσίες διαδικτύου (89,1%), και δημόσια διοίκηση (87,5%). Οι απαντήσαντες θεώρησαν επίσης, σε περίπτωση επιβολής της υποχρέωσης αναφοράς παραβιάσεων της ασφάλειας ΑΔΠ στην αρμόδια εθνική αρχή, ότι τούτο πρέπει να καθοριστεί σε επίπεδο ΕΕ (65,1%) και συμφώνησαν ότι σε αυτήν πρέπει επίσης να υπόκειται η δημόσια διοίκηση (93,5%). Τέλος, οι συμμετέχοντες επιβεβαίωσαν ότι η απαίτηση για εφαρμογή της διαχείρισης των κινδύνων ΑΔΠ σύμφωνα με την εξέλιξη της τεχνολογίας δεν συνεπάγεται για αυτούς σημαντικές επιπλέον δαπάνες (63,4%), και ότι η υποχρέωση αναφοράς παραβιάσεων της ασφάλειας δεν θα επισύρει σημαντικά πρόσθετα έξοδα (72,3%).

Η διαβούλευση με τα κράτη μέλη πραγματοποιήθηκε στο πλαίσιο συναφών συνθέσεων του Συμβουλίου, στο πλαίσιο του ευρωπαϊκού φόρουμ των κρατών μελών (EFMS), στη διάσκεψη για την ασφάλεια στον κυβερνοχώρο, η οποία διοργανώθηκε από την Επιτροπή και από την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, στις 6 Ιουλίου 2012, καθώς και σε ειδικές διμερείς συνεδριάσεις που συγκλήθηκαν έπειτα από αίτηση επιμέρους κρατών μελών.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_el.htm

Πραγματοποιήθηκαν επίσης συζητήσεις με τον ιδιωτικό τομέα, στο πλαίσιο της Ευρωπαϊκής σύμπραξης δημόσιου-ιδιωτικού τομέα για την ανθεκτικότητα [22], αλλά και σε διμερές επίπεδο. Όσον αφορά τον δημόσιο τομέα, η Επιτροπή διεξήγαγε συζητήσεις με τον ENISA και την CERT για τα θεσμικά όργανα της ΕΕ.

2.2. Εκτίμηση του αντίκτυπου

Η Επιτροπή διενήργησε εκτίμηση του αντίκτυπου από τις τρεις επιλογές πολιτικής:

Επιλογή 1: Συνέχιση της σημερινής κατάστασης (βασικό σενάριο) διατήρηση της τρέχουσας προσέγγισης ·

Επιλογή 2: Κανονιστική προσέγγιση, αποτελούμενη από νομοθετική πρόταση για τη θέσπιση κοινού νομικού πλαισίου της ΕΕ για ΑΔΠ όσον αφορά τις ικανότητες του κράτους μέλους, μηχανισμούς συνεργασίας σε επίπεδο ΕΕ, καθώς και απαιτήσεις για βασικούς ιδιωτικούς φορείς και τη δημόσια διοίκηση·

Επιλογή 3: Μεικτή προσέγγιση, η οποία συνδυάζει εθελοντικές πρωτοβουλίες για τις ικανότητες ΑΔΠ του κράτους μέλους και μηχανισμούς για τη συνεργασία σε επίπεδο ΕΕ με κανονιστικές απαιτήσεις για βασικούς ιδιωτικούς φορείς και τη δημόσια διοίκηση.

Η Επιτροπή κατέληξε στο συμπέρασμα ότι η επιλογή 2 θα έχει τον ισχυρότερο θετικό αντίκτυπο, δεδομένου ότι θα βελτιώσει σημαντικά την προστασία των καταναλωτών της ΕΕ, των επιχειρήσεων και των κυβερνήσεων απέναντι σε συμβάντα NIS. Ειδικότερα, οι υποχρεώσεις που επιβάλλονται στα κράτη μέλη θα εξασφαλίσουν επαρκή ετοιμότητα σε εθνικό επίπεδο και θα συμβάλλουν στη δημιουργία κλίματος αμοιβαίας εμπιστοσύνης, που αποτελεί προϋπόθεση για την αποτελεσματική συνεργασία σε επίπεδο ΕΕ. Η θέσπιση μηχανισμών συνεργασίας σε επίπεδο ΕΕ μέσω του δικτύου θα παράσχει συνεκτική και συντονισμένη πρόληψη και αντιμετώπιση των διασυνοριακών συμβάντων και των κινδύνων NIS. Η εισαγωγή απαιτήσεων ως προς την εφαρμογή διαχείρισης κινδύνων ΑΔΠ για τη δημόσια διοίκηση και τους κύριους ιδιωτικούς παράγοντες θα αποτελέσει σημαντικό κίνητρο για την αποτελεσματική διαχείριση των κινδύνων ασφάλειας. Η υποχρέωση αναφοράς των συμβάντων ΑΔΠ με σημαντικό αντίκτυπο θα ενισχύσει την ικανότητα απόκρισης σε συμβάντα και θα προαγάγει τη διαφάνεια. Επιπλέον, βάζοντας τάξη στα του οίκου της, η ΕΕ θα είναι σε θέση να επεκτείνει τη διεθνή της εμβέλεια και να καταστεί ακόμη πιο αξιόπιστος εταίρος για συνεργασία σε διμερές και πολυμερές επίπεδο. Ως εκ τούτου, η ΕΕ θα είναι επίσης σε καλύτερη θέση για να προωθήσει τα θεμελιώδη δικαιώματα και τις θεμελιώδεις αξίες της ΕΕ στο εξωτερικό.

Από την ποσοτική αξιολόγηση προέκυψε ότι η επιλογή 2 δεν συνεπάγεται δυσανάλογη επιβάρυνση για τα κράτη μέλη. Οι δαπάνες για τον ιδιωτικό τομέα θα είναι επίσης περιορισμένες δεδομένου ότι πολλές από τις ενδιαφερόμενες οντότητες αναμένεται ότι θα έχουν ήδη συμμορφωθεί με τις ισχύουσες απαιτήσεις ασφάλειας (δηλ. με την υποχρέωση των υπεύθυνων επεξεργασίας δεδομένων να λαμβάνουν τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα, μεταξύ των οποίων και μέτρα για την ασφάλεια δικτύων και πληροφοριών). Οι υφιστάμενες δαπάνες για την ασφάλεια στον ιδιωτικό τομέα έχουν επίσης ληφθεί υπόψη.

Η παρούσα πρόταση τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, και ιδίως το δικαίωμα στο σεβασμό της ιδιωτικής ζωής και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία του επιχειρείν, το δικαίωμα ιδιοκτησίας, το δικαίωμα αποτελεσματικής ένδικης

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

προστασίας ενώπιον δικαστηρίου και το δικαίωμα ακρόασης. Η οδηγία πρέπει να εφαρμόζεται σύμφωνα με τα εν λόγω δικαιώματα και αρχές.

3. ΝΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΠΡΟΤΑΣΗΣ

3.1. Νομική βάση

Η Ευρωπαϊκή Ένωση έχει εξουσιοδοτηθεί να θεσπίζει τα μέτρα που αποβλέπουν στην εγκαθίδρυση ή στη διασφάλιση της λειτουργίας της εσωτερικής αγοράς, σύμφωνα με τις οικείες διατάξεις των Συνθηκών (άρθρο 26 της συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης – ΣΛΕΕ). Σύμφωνα με το άρθρο 114 της ΣΛΕΕ, η ΕΕ μπορεί να θεσπίζει «μέτρα σχετικά με την *προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών* που έχουν ως αντικείμενο την εγκαθίδρυση και τη λειτουργία της εσωτερικής αγοράς».

Όπως προαναφέρθηκε, τα συστήματα δικτύων και πληροφοριών διαδραματίζουν ουσιαστικό ρόλο στη διευκόλυνση της διασυνοριακής κυκλοφορίας των εμπορευμάτων, των υπηρεσιών και των προσώπων. Συχνά είναι διασυνδεμένα, ενώ το διαδίκτυο έχει παγκόσμιο χαρακτήρα. Με δεδομένη αυτή την εγγενή διακρατική διάσταση, μια διαταραχή σε ένα κράτος μέλος μπορεί επίσης να επηρεάσει και άλλα κράτη μέλη, καθώς και την ΕΕ στο σύνολό της. Η ανθεκτικότητα και η σταθερότητα των συστημάτων δικτύων και πληροφοριών είναι επομένως ουσιώδης για την ομαλή λειτουργία της εσωτερικής αγοράς.

Ο ενωσιακός νομοθέτης έχει ήδη αναγνωρίσει την ανάγκη εναρμόνισης των κανόνων που αφορούν την ασφάλεια δικτύων και πληροφοριών, προκειμένου να διασφαλίσει την ανάπτυξη της εσωτερικής αγοράς. Ειδικότερα, αυτό ίσχυε στην περίπτωση του κανονισμού 460/2004 για τη δημιουργία του ENISA[23], που βασίζεται στο άρθρο 114 της ΣΛΕΕ.

Οι διαφορές που προκύπτουν από άνισες εθνικές ικανότητες, πολιτικές και επίπεδο προστασίας ΑΔΠ σε όλα τα κράτη μέλη, έχουν ως αποτέλεσμα να δημιουργούνται εμπόδια στην εσωτερική αγορά και δικαιολογούν την ανάληψη δράσης σε επίπεδο ΕΕ.

3.2. Επικουρικότητα

Η ευρωπαϊκή παρέμβασης στο πεδίο της ασφάλειας δικτύων και πληροφοριών είναι δικαιολογημένη με βάση την αρχή της επικουρικότητας.

Πρώτον, δεδομένου του διασυνοριακού χαρακτήρα της NIS, η απουσία παρέμβασης σε επίπεδο ΕΕ θα οδηγούσε σε μια κατάσταση όπου κάθε κράτος μέλος θα ενεργούσε μεμονωμένα, αγνοώντας τις αλληλεξαρτήσεις μεταξύ συστημάτων και δικτύων πληροφοριών στην ΕΕ. Η διασφάλιση επαρκούς βαθμού συντονισμού μεταξύ των κρατών μελών θα εγγυούνταν σωστή διαχείριση των κινδύνων για την ασφάλεια δικτύων και πληροφοριών στο διασυνοριακό πλαίσιο εντός του οποίου ανακύπτουν. Οι αποκλίσεις στους κανονισμούς NIS αποτελούν εμπόδιο για τις επιχειρήσεις που επιθυμούν να δραστηριοποιούνται σε περισσότερες από μία χώρες, καθώς και για την επίτευξη παγκόσμιων οικονομιών κλίμακας.

Δεύτερον, απαιτούνται κανονιστικές υποχρεώσεις σε επίπεδο ΕΕ ώστε να προκύψουν ισότιμοι όροι ανταγωνισμού και να γεφυρωθούν τα νομοθετικά κενά. Η καθαρά εθελοντική προσέγγιση είχε ως αποτέλεσμα τη συνεργασία μόνο μιας μειοψηφίας κρατών μελών με υψηλό επίπεδο ικανοτήτων. Προκειμένου να εμπλακούν όλα τα κράτη μέλη, είναι απαραίτητο να εξασφαλιστεί ότι όλα διαθέτουν το απαιτούμενο ελάχιστο επίπεδο ικανοτήτων. Τα μέτρα για την ασφάλεια δικτύων και πληροφοριών που θεσπίζουν οι

[23] Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ΕΕ L 77 της 13.03.2004, σ. 1).

κυβερνήσεις πρέπει να είναι συνεπή μεταξύ τους και να είναι συντονισμένα, με σκοπό την περιστολή και ελαχιστοποίηση των επιπτώσεων από συμβάντα ΑΔΠ. Εντός του δικτύου, μέσω ανταλλαγής βέλτιστης πρακτικής και με τη συνεχή συμμετοχή του ENISA, οι αρμόδιες αρχές και η Επιτροπή θα συνεργάζονται για να διευκολύνουν την συγκλίνουσα εφαρμογή της οδηγίας σε όλη την ΕΕ. Επιπλέον, οι συντονισμένες δράσεις πολιτικής στην ασφάλεια δικτύων και πληροφοριών (ΑΔΠ) μπορεί να έχουν ισχυρό θετικό αντίκτυπο στην αποτελεσματική προστασία των θεμελιωδών δικαιωμάτων και ειδικά στο δικαίωμα της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής. Επομένως, η δράση σε επίπεδο ΕΕ θα βελτιώσει την αποτελεσματικότητα των υφιστάμενων εθνικών πολιτικών και θα διευκολύνει την ανάπτυξή τους.

Τα προτεινόμενα μέτρα είναι επίσης δικαιολογημένα για λόγους αναλογικότητας. Οι απαιτήσεις που αφορούν τα κράτη μέλη καθορίζονται στο ελάχιστο αναγκαίο επίπεδο για την επίτευξη επαρκούς ετοιμότητας και για να καταστεί δυνατή η συνεργασία που θα βασίζεται στην εμπιστοσύνη. Αυτό παρέχει επίσης στα κράτη μέλη τη δυνατότητα να λάβουν δεόντως υπόψη τις εθνικές ιδιαιτερότητες και εξασφαλίζει ότι οι κοινές αρχές της ΕΕ εφαρμόζονται κατά τρόπο αναλογικό. Το ευρύ πεδίο εφαρμογής θα επιτρέψει στα κράτη μέλη να εφαρμόσουν την οδηγία υπό το φως των πραγματικών κινδύνων που αντιμετωπίζουν σε εθνικό επίπεδο, όπως προσδιορίζονται στην εθνική στρατηγική ΑΔΠ. Οι απαιτήσεις για εφαρμογή της διαχείρισης κινδύνων αφορούν αποκλειστικά οντότητες ζωτικής σημασίας και επιβάλλουν μέτρα αναλογικά προς τους κινδύνους. Η δημόσια διαβούλευση υπογράμμισε τη σημασία που έχει η εγγύηση της ασφάλειας αυτών των κρίσιμων οντοτήτων. Οι απαιτήσεις υποβολής εκθέσεων θα αφορούν μόνο συμβάντα με σημαντικό αντίκτυπο. Όπως αναφέρθηκε παραπάνω, τα μέτρα δεν συνεπάγονται δυσανάλογο κόστος, δεδομένου ότι πολλές από αυτές τις οντότητες, ως υπεύθυνοι επεξεργασίας των δεδομένων, υποχρεούνται ήδη βάσει των ισχυόντων κανόνων προστασίας των δεδομένων να διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Προκειμένου να μην επιβληθεί δυσανάλογο βάρος στις μικρές επιχειρήσεις, ιδίως στις ΜΜΕ, οι απαιτήσεις είναι ανάλογες προς τον κίνδυνο που παρουσιάζουν τα σχετικά συστήματα δικτύων και πληροφοριών και δεν πρέπει να εφαρμόζονται σε πολύ μικρές επιχειρήσεις Οι κίνδυνοι πρέπει να προσδιορίζονται εν πρώτοις από τις οντότητες που υπόκεινται στις εν λόγω υποχρεώσεις, και οι οποίες θα πρέπει να αποφασίζουν σχετικά με τα εφαρμοστέα μέτρα για περιορισμό των κινδύνων αυτών.

Οι δηλωμένοι στόχοι μπορούν να επιτευχθούν καλύτερα σε επίπεδο ΕΕ και όχι μεμονωμένα από τα κράτη μέλη, λαμβανομένων υπόψη των διασυνοριακών πτυχών των συμβάντων και κινδύνων ΑΔΠ . Κατά συνέπεια, η Ένωση μπορεί να θεσπίζει μέτρα σύμφωνα με την αρχή της επικουρικότητας που ορίζεται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας, η προτεινόμενη οδηγία δεν υπερβαίνει ό, τι είναι απαραίτητο για την επίτευξη αυτών των στόχων.

Για το σκοπό της επίτευξης των στόχων, η Επιτροπή πρέπει να εξουσιοδοτηθεί να εγκρίνει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, ώστε να συμπληρώνει ή να τροποποιεί ορισμένα μη ουσιώδη στοιχεία της βασικής πράξης. Με την πρόταση της Επιτροπής επιδιώκεται επίσης να στηριχτεί η διαδικασία της αναλογικότητας κατά την εφαρμογή των υποχρεώσεων που επιβάλλονται σε ιδιωτικούς και δημόσιους φορείς.

Προκειμένου να διασφαλιστούν ομοιόμορφοι όροι για την εφαρμογή της βασικής πράξης, πρέπει να εξουσιοδοτηθεί η Επιτροπή να εκδίδει εκτελεστικές πράξεις σύμφωνα με το άρθρο 291 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

Λαμβάνοντας υπόψη ιδίως το ευρύτερο πεδίο εφαρμογής της προτεινόμενης οδηγίας, το γεγονός ότι άπτεται τομέων που αποτελούν αντικείμενο εκτεταμένων νομοθετικών ρυθμίσεων, καθώς και τις νομικές υποχρεώσεις που απορρέουν από το οικείο κεφάλαιο IV, η κοινοποίηση των μέτρων μεταφοράς στο εθνικό δίκαιο πρέπει να συνοδεύεται από επεξηγηματικά έγγραφα. Σύμφωνα με την κοινή πολιτική δήλωση των κρατών μελών και της Επιτροπής, της 28ης Σεπτεμβρίου 2011, σχετικά με τα επεξηγηματικά έγγραφα, τα κράτη μέλη έχουν αναλάβει την υποχρέωση, σε αιτιολογημένες περιπτώσεις, να συνοδεύουν την κοινοποίηση των μέτρων μεταφοράς στο εθνικό δίκαιο με ένα ή περισσότερα έγγραφα που επεξηγούν τη σχέση ανάμεσα στα συστατικά στοιχεία μιας οδηγίας και στα αντίστοιχα μέρη των νομικών πράξεων μεταφοράς στο εθνικό δίκαιο. Όσον αφορά την παρούσα οδηγία, ο νομοθέτης κρίνει ότι είναι αιτιολογημένη η διαβίβαση των εγγράφων αυτών.

4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών πρέπει να υποστηρίζονται από ασφαλή υποδομή. Η πρόταση θα έχει επιπτώσεις στον προϋπολογισμό της ΕΕ μόνον εφόσον τα κράτη μέλη επιλέξουν την προσαρμογή μιας υπάρχουσας υποδομής (π.χ. sTESTA) και αναθέσουν στην Επιτροπή την υλοποίησή της βάσει του ΠΔΠ 2014-2020. Το εφάπαξ κόστος εκτιμάται σε 1.250.000 ευρώ και αναλαμβάνεται από τον προϋπολογισμό της ΕΕ, στο κονδύλιο 09.03.02 (για την προώθηση της επιγραμμικής διασύνδεσης και διαλειτουργικότητας των εθνικών δημόσιων υπηρεσιών, καθώς και της πρόσβασης σε αυτά τα δίκτυα — κεφάλαιο 09.03, CEF, Διευκόλυνση *«Συνδέοντας την Ευρώπη»* — τηλεπικοινωνιακά δίκτυα) υπό τον όρο ότι είναι διαθέσιμα επαρκή κονδύλια βάσει της CEF. Εναλλακτικά, τα κράτη μέλη μπορούν είτε να μοιράζονται το εφάπαξ κόστος προσαρμογής υφιστάμενης υποδομής είτε να αποφασίσουν να ιδρύσουν μια νέα υποδομή και να αναλάβουν το κόστος, που εκτιμάται σε περίπου 10 εκατ. ευρώ το χρόνο.

2013/0027 (COD)

Πρόταση

ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

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

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

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

Κατόπιν διαβούλευσης με τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Τα συστήματα και οι υπηρεσίες δικτύων και πληροφοριών διαδραματίζουν ζωτικό ρόλο στην κοινωνία. Η αξιοπιστία και η ασφάλειά τους είναι ουσιαστικής σημασίας για τις οικονομικές δραστηριότητες και την κοινωνική ευημερία, και ιδίως για τη λειτουργία της εσωτερικής αγοράς.

(2) Το μέγεθος και η συχνότητα σκόπιμων ή τυχαίων συμβάντων ασφάλειας αυξάνεται και συνιστά μείζονα απειλή για τη λειτουργία των δικτύων και των συστημάτων πληροφοριών. Τέτοια συμβάντα μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σημαντική ζημία στην οικονομία της Ένωσης.

(3) Ως μέσο επικοινωνίας χωρίς σύνορα, τα ψηφιακά συστήματα πληροφοριών και κυρίως το διαδίκτυο διαδραματίζουν ουσιαστικό ρόλο στη διευκόλυνση της διασυνοριακής κυκλοφορίας εμπορευμάτων, υπηρεσιών και προσώπων. Λόγω του διακρατικού χαρακτήρα, ενδεχόμενη σημαντική διαταραχή των συστημάτων αυτών σε ένα κράτος μέλος μπορεί επίσης να επηρεάσει και άλλα κράτη μέλη και την Ένωση στο σύνολό της. Η ανθεκτικότητα και η σταθερότητα των συστημάτων δικτύων και πληροφοριών είναι επομένως ουσιώδης για την ομαλή λειτουργία της εσωτερικής αγοράς.

(4) Ένας μηχανισμός συνεργασίας πρέπει να δημιουργηθεί σε επίπεδο Ένωσης ώστε να καταστεί δυνατή η ανταλλαγή πληροφοριών και η συντονισμένη ανίχνευση και αντιμετώπιση όσον αφορά την ασφάλεια δικτύων και πληροφοριών («NIS»). Για να είναι αποτελεσματικός και χωρίς αποκλεισμούς ο εν λόγω μηχανισμός, είναι σημαντικό όλα τα κράτη μέλη να διαθέτουν ένα ελάχιστο επίπεδο ικανοτήτων καθώς

[1] ΕΕ C […] της […], σ. […].

και μια στρατηγική που θα εξασφαλίζει υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών στην επικράτειά τους. Πρέπει επίσης να ισχύουν ελάχιστες απαιτήσεις ασφάλειας και για τη δημόσια διοίκηση και τους φορείς εκμετάλλευσης των υποδομών πληροφοριών ζωτικής σημασίας για την προαγωγή πνεύματος διαχείρισης κινδύνων και για να διασφαλιστεί η αναφορά των σοβαρότερων συμβάντων.

(5) Για να καλυφθούν όλα τα σχετικά συμβάντα και οι σχετικοί κίνδυνοι, η παρούσα οδηγία πρέπει να ισχύσει για όλα τα συστήματα δικτύων και πληροφοριών. Οι υποχρεώσεις των δημόσιων διοικήσεων και των φορέων της αγοράς δεν πρέπει, ωστόσο, να ισχύσουν για τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών κατά την έννοια της οδηγίας 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο)[2], οι οποίες υπόκεινται στις ειδικές απαιτήσεις ακεραιότητας και ασφάλειας που ορίζονται στο άρθρο 13α της εν λόγω οδηγίας ούτε πρέπει να ισχύσουν για παρόχους υπηρεσιών εμπιστοσύνης.

(6) Οι υφιστάμενες ικανότητες δεν επαρκούν για να εξασφαλιστεί ένα υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών (ΑΔΠ) εντός της Ένωσης. Τα κράτη μέλη έχουν πολύ διαφορετικά επίπεδα ετοιμότητας, με αποτέλεσμα κατακερματισμένες προσεγγίσεις σε ολόκληρη την Ένωση. Αυτό οδηγεί σε άνισο επίπεδο προστασίας καταναλωτών και επιχειρήσεων, ενώ υπονομεύει το συνολικό επίπεδο ΑΔΠ εντός της Ένωσης. Η απουσία κοινών ελάχιστων απαιτήσεων για τη δημόσια διοίκηση και τους φορείς της αγοράς, καθιστά εξάλλου αδύνατο να συσταθεί ένας σφαιρικός και αποτελεσματικός μηχανισμός για συνεργασία σε επίπεδο Ένωσης.

(7) Η αποτελεσματική απόκριση στα προβλήματα ασφάλειας των συστημάτων δικτύων και πληροφοριών απαιτεί, συνεπώς, σφαιρική προσέγγιση σε επίπεδο Ένωσης που να καλύπτει κοινές ελάχιστες απαιτήσεις δημιουργίας ικανοτήτων και σχεδιασμού, ανταλλαγής πληροφοριών και συντονισμού ενεργειών, καθώς και κοινές ελάχιστες απαιτήσεις ασφάλειας για όλους τους ενδιαφερόμενους φορείς της αγοράς και για τη δημόσια διοίκηση.

(8) Οι διατάξεις της παρούσας οδηγίας δεν πρέπει να θίγουν τη δυνατότητα κάθε κράτους μέλους να λαμβάνει τα αναγκαία μέτρα για την προστασία των ουσιαστικών συμφερόντων του στον τομέα της ασφάλειας και για την εξασφάλιση της δημόσιας τάξης και ασφάλειας, καθώς και να διευκολύνει τη διερεύνηση, εξιχνίαση και δίωξη ποινικών αδικημάτων. Σύμφωνα με το άρθρο 346 της ΣΛΕΕ, κανένα κράτος μέλος δεν πρέπει να υποχρεώνεται να παρέχει πληροφορίες, τη διάδοση των οποίων θεωρεί αντίθετη προς τα ουσιώδη συμφέροντα ασφάλειάς του.

(9) Για την επίτευξη και τη διατήρηση κοινού υψηλού επιπέδου ασφάλειας των δικτύων και των συστημάτων πληροφοριών, κάθε κράτος μέλος πρέπει να διαθέτει εθνική στρατηγική ΑΔΠ που να καθορίζει τους στρατηγικούς στόχους και τις συγκεκριμένες δράσεις πολιτικής που πρέπει να εφαρμοστούν. Πρέπει να εκπονηθούν σε εθνικό επίπεδο σχέδια συνεργασίας ΑΔΠ που να συμμορφώνονται με τις βασικές απαιτήσεις προκειμένου να επιτευχθούν επίπεδα ικανότητας απόκρισης που να επιτρέπουν αποτελεσματική και αποδοτική συνεργασία σε εθνικό και σε ενωσιακό επίπεδο σε περίπτωση συμβάντων.

(10) Για να καταστεί δυνατή η αποτελεσματική υλοποίηση των διατάξεων που θεσπίζονται δυνάμει της παρούσας οδηγίας, πρέπει να συσταθεί ή να οριστεί σε κάθε κράτος μέλος

[2] ΕΕ L 108 της 24.04.2002, σ. 33.

ένας φορέας υπεύθυνος για τον συντονισμό θεμάτων ΑΔΠ και για να ενεργεί ως εστιακό σημείο για διασυνοριακή συνεργασία σε επίπεδο Ένωσης . Στους εν λόγω φορείς πρέπει να δοθούν επαρκείς τεχνικοί, οικονομικοί και ανθρώπινοι πόροι ώστε να εξασφαλιστεί ότι θα μπορούν να εκτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους έχουν ανατεθεί επιτυγχάνοντας, συνεπώς, τους στόχους της παρούσας οδηγίας.

(11) Όλα τα κράτη μέλη πρέπει να διαθέτουν τον κατάλληλο εξοπλισμό, τόσο σε τεχνικές όσο και σε οργανωτικές ικανότητες, για την πρόληψη, τον εντοπισμό, την αντιμετώπιση και τον μετριασμό των συμβάντων και κινδύνων σε συστήματα δικτύων και πληροφοριών. Κατά συνέπεια, πρέπει να ιδρυθούν σε όλα τα κράτη μέλη εύρυθμα λειτουργούσες ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) που να συμμορφώνονται με τις βασικές απαιτήσεις, ώστε να διασφαλίζονται αποτελεσματικές και συμβατές ικανότητες για την αντιμετώπιση συμβάντων και κινδύνων και να εξασφαλίζεται αποτελεσματική συνεργασία σε ενωσιακό επίπεδο.

(12) Αξιοποιώντας τη σημαντική πρόοδο που έχει σημειωθεί στο πλαίσιο του ευρωπαϊκού φόρουμ των κρατών μελών (EFMS) στην προώθηση συζητήσεων και ανταλλαγών όσον αφορά ορθές πολιτικές πρακτικές, συμπεριλαμβανομένης της επεξεργασίας αρχών για την ευρωπαϊκή συνεργασία για την αντιμετώπιση της κρίσης στον κυβερνοχώρο, τα κράτη μέλη και η Επιτροπή πρέπει να συγκροτήσουν δίκτυο μόνιμης επικοινωνίας και υποστήριξης της συνεργασίας μεταξύ τους. Αυτός ο ασφαλής και αποτελεσματικός μηχανισμός συνεργασίας πρέπει να καταστήσει δυνατή τη δομημένη και συντονισμένη ανταλλαγή πληροφοριών, καθώς και τον εντοπισμό και την απόκριση σε ενωσιακό επίπεδο.

(13) Ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών (ENISA) πρέπει να συνδράμει τα κράτη μέλη και την Επιτροπή, παρέχοντας την εμπειρογνωμοσύνη και τις συμβουλές του, καθώς και διευκολύνοντας την ανταλλαγή βέλτιστης πρακτικής. Ειδικότερα, κατά την εφαρμογή της παρούσας οδηγίας, η Επιτροπή πρέπει να συμβουλευτεί τον ENISA. Προκειμένου να διασφαλίζεται αποτελεσματική και έγκαιρη ενημέρωση των κρατών μελών και της Επιτροπής, πρέπει να κοινοποιούνται εντός του δικτύου συνεργασίας έγκαιρες προειδοποιήσεις για συμβάντα και κινδύνους. Για την ανάπτυξη ικανοτήτων και γνώσεων μεταξύ των κρατών μελών, πρέπει το δίκτυο συνεργασίας να χρησιμεύει επίσης ως μέσο για την ανταλλαγή ορθής πρακτικής, να επικουρεί τα μέλη του όσον αφορά την ανάπτυξη ικανοτήτων, να κατευθύνει τη διοργάνωση αξιολογήσεων από ομοτίμους και ασκήσεωνε σχετικά με την ασφάλεια δικτύων και πληροφοριών.

(14) Πρέπει να τεθεί σε εφαρμογή μια υποδομή για ασφαλή ανταλλαγή πληροφοριών προκειμένου να καταστεί δυνατή η ανταλλαγή ευαίσθητων και εμπιστευτικών πληροφοριών εντός του δικτύου συνεργασίας. Με την επιφύλαξη της υποχρέωσής τους για κοινοποίηση στο δίκτυο συνεργασίας συμβάντων και κινδύνων ενωσιακής διάστασης, η πρόσβαση σε πληροφορίες εμπιστευτικού χαρακτήρα από άλλα κράτη μέλη πρέπει να χορηγείται στα κράτη μέλη μόνον εφόσον έχει καταδειχθεί ότι οι τεχνικοί, οικονομικοί και ανθρώπινοι πόροι και οι διαδικασίες τους, καθώς και η επικοινωνιακή υποδομή τους, εγγυώνται την αποτελεσματική, αποδοτική και ασφαλή συμμετοχή τους στο δίκτυο.

(15) Δεδομένου ότι τα περισσότερα συστήματα δικτύων και πληροφοριών είναι ιδιωτικά, η συνεργασία μεταξύ του ιδιωτικού και του δημόσιου τομέα έχει ουσιώδη σημασία. Οι παράγοντες της αγοράς πρέπει να παροτρύνονται να διατηρούν τους δικούς τους άτυπους μηχανισμούς συνεργασίας για την εξασφάλιση της ασφάλειας δικτύων και

πληροφοριών. Πρέπει επίσης να συνεργάζονται με τον δημόσιο τομέα και να ανταλλάσσουν πληροφορίες και βέλτιστη πρακτική έναντι επιχειρησιακής στήριξης σε περίπτωση συμβάντων.

(16) Προκειμένου να διασφαλιστεί η διαφάνεια και η καλή ενημέρωση των πολιτών της ΕΕ και των φορέων της αγοράς, πρέπει οι αρμόδιες αρχές να συγκροτήσουν κοινό ιστότοπο για τη δημοσίευση μη εμπιστευτικών πληροφοριών σχετικά με συμβάντα και κινδύνους.

(17) Εάν οι πληροφορίες θεωρούνται εμπιστευτικές σύμφωνα με τους ενωσιακούς και εθνικούς κανόνες περί επιχειρηματικού απορρήτου, πρέπει η εμπιστευτικότητα αυτή να εξασφαλίζεται κατά την άσκηση των δραστηριοτήτων και την εκπλήρωση των στόχων της παρούσας οδηγίας.

(18) Ιδίως με βάση τις εθνικές εμπειρίες διαχείρισης κρίσεων και σε συνεργασία με τον ENISA, η Επιτροπή και τα κράτη μέλη πρέπει να εκπονήσουν ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ όπου θα καθορίζονται μηχανισμοί συνεργασίας για την αντιμετώπιση κινδύνων και συμβάντων. Το εν λόγω σχέδιο πρέπει να λαμβάνεται δεόντως υπόψη για τον χειρισμό έγκαιρων προειδοποιήσεων εντός του δικτύου συνεργασίας.

(19) Κοινοποίηση έγκαιρης προειδοποίησης στο πλαίσιο του δικτύου πρέπει να απαιτείται μόνον όταν η κλίμακα και η σοβαρότητα του σχετικού συμβάντος ή κινδύνου είναι ή μπορούν να καταστούν τόσο σημαντικές ώστε να είναι απαραίτητες πληροφορίες ή συντονισμός της απόκρισης σε ενωσιακό επίπεδο. Οι έγκαιρες προειδοποιήσεις πρέπει, επομένως, να περιορίζονται σε πραγματικά ή δυνητικά συμβάντα ή σε κινδύνους που αναπτύσσονται ταχέως, υπερβαίνουν τις εθνικές ικανότητες απόκρισης ή πλήττουν περισσότερα του ενός κράτη μέλη. Για να καταστεί δυνατή η ορθή αξιολόγηση, πρέπει όλες οι σχετικές πληροφορίες για την αξιολόγηση του κινδύνου ή του συμβάντος να κοινοποιούνται στο δίκτυο συνεργασίας.

(20) Με την παραλαβή μιας έγκαιρης προειδοποίησης και την αξιολόγησή της, πρέπει οι αρμόδιες αρχές να συμφωνήσουν σχετικά με συντονισμένη απόκριση, σύμφωνα με το ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ. Οι αρμόδιες αρχές καθώς και η Επιτροπή πρέπει να ενημερώνονται σχετικά με τα μέτρα που λαμβάνονται σε εθνικό επίπεδο ως αποτέλεσμα της συντονισμένης απόκρισης.

(21) Δεδομένου του παγκόσμιου χαρακτήρα των προβλημάτων ΑΔΠ, υπάρχει ανάγκη στενότερης διεθνούς συνεργασίας για τη βελτίωση των προτύπων ασφάλειας και της ανταλλαγής πληροφοριών, καθώς και για την προώθηση κοινής σφαιρικής προσέγγισης των θεμάτων ασφάλειας δικτύων και πληροφοριών.

(22) Αρμοδιότητες για την εξασφάλιση ΑΔΠ υπέχουν σε μεγάλο βαθμό η δημόσια διοίκηση και οι φορείς της αγοράς. Με κατάλληλες κανονιστικές απαιτήσεις και εθελοντικές κλαδικές πρακτικές πρέπει να προωθηθεί και να αναπτυχθεί πνεύμα διαχείρισης κινδύνων, περιλαμβάνοντας εκτίμηση των κινδύνων και εφαρμογή ενδεδειγμένων μέτρων ασφάλειας για τους κινδύνους που αντιμετωπίζουν οι επιχειρήσεις. Η εξασφάλιση ίσων όρων ανταγωνισμού είναι επίσης απαραίτητη για την αποτελεσματική λειτουργία του δικτύου συνεργασίας ώστε να εξασφαλίζεται αποτελεσματική συνεργασία από όλα τα κράτη μέλη.

(23) Στην οδηγία 2002/21/ΕΚ ορίζεται ότι οι επιχειρήσεις παροχής δημοσίων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών λαμβάνουν τα κατάλληλα μέτρα για τη διασφάλιση της ακεραιότητας και ασφάλειάς τους, ενώ εισάγονται απαιτήσεις κοινοποίησης παραβιάσεων της

ασφάλειας και απώλειας της ακεραιότητας. Στην οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)[3] απαιτείται από τον πάροχο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διαφυλάσσεται η ασφάλεια των υπηρεσιών του.

(24) Οι εν λόγω υποχρεώσεις πρέπει να επεκταθούν πέρα από τον τομέα των ηλεκτρονικών επικοινωνιών σε βασικούς παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, όπως ορίζεται στην οδηγία 98/34/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Ιουνίου 1998, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και κανονισμών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών[4], που ενισχύουν κατάντη υπηρεσίες της κοινωνίας της πληροφορίας ή επιγραμμικές δραστηριότητες όπως οι πλατφόρμες ηλ-εμπορίου, πύλες πληρωμών μέσω διαδικτύου, κοινωνικά δίκτυα, μηχανές αναζήτησης, υπηρεσίες υπολογιστικού νέφους, καταστήματα ηλεκτρονικών εφαρμογών. Ενδεχόμενη διαταραχή αυτών των υπηρεσιών γενικής εφαρμογής της κοινωνίας της πληροφορίας αποκλείει την παροχή άλλων υπηρεσιών της κοινωνίας της πληροφορίας που βασίζονται σε αυτές ως παραμέτρων βασικής σημασίας. Οι σχεδιαστές λογισμικού και κατασκευαστές υλισμικού δεν είναι πάροχοι υπηρεσιών της κοινωνίας της πληροφορίας και, ως εκ τούτου, εξαιρούνται. Οι υποχρεώσεις αυτές πρέπει επίσης να επεκταθούν στη δημόσια διοίκηση και στους φορείς εκμετάλλευσης υποδομών ζωτικής σημασίας, που στηρίζονται σε μεγάλο βαθμό στις τεχνολογίες της πληροφορίας και των επικοινωνιών και που είναι απαραίτητες για τη διατήρηση ζωτικών οικονομικών ή κοινωνικών λειτουργιών όπως η ηλεκτρική ενέργεια και το φυσικό αέριο, οι μεταφορές, τα πιστωτικά ιδρύματα, το χρηματιστήριο και η υγεία. Ενδεχόμενη διαταραχή των εν λόγω συστημάτων δικτύων και πληροφοριών θα πλήξει την εσωτερική αγορά.

(25) Τα τεχνικά και οργανωτικά μέτρα που έχουν επιβληθεί στη δημόσια διοίκηση και στους φορείς της αγοράς δεν πρέπει να συνεπάγονται ότι συγκεκριμένα εμπορικά προϊόντα τεχνολογίας πληροφοριών και επικοινωνιών θα σχεδιάζονται, θα αναπτύσσονται ή θα παράγονται με συγκεκριμένο τρόπο.

(26) Η δημόσια διοίκηση και οι φορείς της αγοράς πρέπει να εγγυώνται την ασφάλεια των δικτύων και συστημάτων που υπάγονται στον έλεγχό τους. Κατά κύριο λόγο θα πρόκειται για ιδιωτικά δίκτυα και συστήματα τα οποία είτε τελούν υπό τη διαχείριση του εσωτερικού τους προσωπικού μηχανογράφησης είτε η ασφάλεια των οποίων έχει ανατεθεί σε εξωτερικούς συνεργάτες. Οι υποχρεώσεις κοινοποίησης και ασφάλειας πρέπει να ισχύουν για τους αρμόδιους φορείς της αγοράς και για τη δημόσια διοίκηση, ανεξάρτητα από το αν εκτελούν τη συντήρηση των δικτύων και των συστημάτων πληροφοριών τους στο εσωτερικό ή αν την αναθέτουν σε τρίτους.

(27) Προκειμένου να μην επιβληθεί δυσανάλογο οικονομικό και διοικητικό βάρος στις μικρές επιχειρήσεις και στους χρήστες, οι απαιτήσεις πρέπει να είναι ανάλογες προς τον κίνδυνο που συνιστά το σχετικό δίκτυο ή το σύστημα πληροφοριών, λαμβάνοντας υπόψη το επίπεδο της τεχνολογίας των μέτρων αυτών. Οι απαιτήσεις αυτές δεν πρέπει να εφαρμόζονται σε πολύ μικρές επιχειρήσεις.

---

[3] ΕΕ L 201 της 31.07.2002, σ. 37.

[4] ΕΕ L 204 της 21.07.1998, σ. 37.

(28) Οι αρμόδιες αρχές πρέπει να δώσουν τη δέουσα προσοχή στη διατήρηση άτυπων και αξιόπιστων δικτύων ανταλλαγής πληροφοριών μεταξύ των διαφόρων φορέων της αγοράς και μεταξύ του δημόσιου και του ιδιωτικού τομέα. Κατά τη δημοσίευση των συμβάντων που κοινοποιούνται στις αρμόδιες αρχές πρέπει να αντισταθμίζονται δεόντως το συμφέρον του κοινού για ενημέρωση σχετικά με απειλές αφενός με τους πιθανούς κινδύνους για την υπόληψη και εμπορικές ζημίες για τη δημόσια διοίκηση και τους φορείς της αγοράς που κοινοποιούν συμβάντα αφετέρου. Κατά την εφαρμογή των υποχρεώσεων κοινοποίησης, οι αρμόδιες αρχές πρέπει να λάβουν ιδιαιτέρως υπόψη την ανάγκη να διατηρηθεί ο αυστηρά εμπιστευτικός χαρακτήρας των πληροφοριών ως προς τα τρωτά σημεία των προϊόντων πριν από την έκδοση των αντίστοιχων διορθωτικών ρυθμίσεων ασφάλειας.

(29) Οι αρμόδιες αρχές πρέπει να διαθέτουν τα απαραίτητα μέσα για την εκτέλεση των καθηκόντων τους, συμπεριλαμβανομένων και εξουσιών επαρκούς πληροφόρησης από τους φορείς της αγοράς και τη δημόσια διοίκηση ώστε να αξιολογήσουν το επίπεδο ασφάλειας των συστημάτων δικτύων και πληροφοριών, καθώς και αξιόπιστων και περιεκτικών δεδομένων σχετικά με τα πραγματικά συμβάντα που είχαν αντίκτυπο στην λειτουργία των συστημάτων δικτύων και πληροφοριών.

(30) Συχνά, τα συμβάντα ανάγονται σε αξιόποινες δραστηριότητες. Υπόνοιες ως προς τον ποινικό χαρακτήρα των συμβάντων μπορεί να υπάρχουν ακόμη και αν τα αποδεικτικά στοιχεία για την τεκμηρίωσή του μπορεί να μην είναι εξαρχής αρκετά σαφή. Στο πλαίσιο αυτό, η κατάλληλη συνεργασία μεταξύ των αρμοδίων αρχών και των αρχών επιβολής του νόμου πρέπει να συνιστά μέρος μιας αποτελεσματικής και ολοκληρωμένης απόκρισης σε απειλές συμβάντων που θέτουν σε κίνδυνο την ασφάλεια. Ειδικότερα, η προαγωγή ασφαλούς, προστατευμένου και ανθεκτικότερου περιβάλλοντος απαιτεί συστηματική αναφορά στις αρχές επιβολής του νόμου των ύποπτων συμβάντων σοβαρού ποινικού χαρακτήρα. Ο σοβαρός ποινικός χαρακτήρας των συμβάντων πρέπει να αξιολογείται υπό το πρίσμα της ενωσιακής νομοθεσίας για το ηλεκτρονικό έγκλημα.

(31) Ως αποτέλεσμα συμβάντων, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές και οι αρχές προστασίας δεδομένων πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες σε όλα τα συναφή θέματα για την αντιμετώπιση των παραβιάσεων σε προσωπικά δεδομένα που οφείλονται σε συμβάντα. Τα κράτη μέλη θέτουν σε εφαρμογή την υποχρέωση κοινοποίησης συμβάντων ασφάλειας κατά τρόπο που να ελαχιστοποιεί τον διοικητικό φόρτο σε περίπτωση που το συμβάν ασφάλειας είναι επίσης παραβίαση προσωπικών δεδομένων, σύμφωνα με τον κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών[5]. Σε συνεννόηση με τις αρμόδιες αρχές και τις αρχές προστασίας δεδομένων, ο ENISA θα μπορούσε να βοηθήσει με την ανάπτυξη μηχανισμών και προτύπων ανταλλαγής πληροφοριών, αποφεύγοντας την ανάγκη ύπαρξης δύο προτύπων κοινοποίησης. Το ενιαίο αυτό πρότυπο κοινοποίησης θα διευκόλυνε την αναφορά των συμβάντων όπου διακυβεύονται παραβιάσεις προσωπικών δεδομένων, συμβάλλοντας έτσι σε ελάφρυνση του διοικητικού φόρτου για τις επιχειρήσεις και τη δημόσια διοίκηση.

(32) Η τυποποίηση των απαιτήσεων ασφάλειας είναι διαδικασία καθοδηγούμενη από την αγορά. Προκειμένου να εξασφαλιστεί συγκλίνουσα εφαρμογή των προτύπων

[5] SEC(2012) 72 τελικό

ασφάλειας, τα κράτη μέλη πρέπει να ενθαρρύνουν τη συμμόρφωση με καθορισμένα πρότυπα, ώστε να κατοχυρωθεί υψηλό επίπεδο ασφάλειας σε ενωσιακό επίπεδο. Για το σκοπό αυτό, μπορεί να είναι αναγκαία η κατάρτιση εναρμονισμένων προτύπων, που πρέπει να γίνει σύμφωνα με τον κανονισμό(ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, που τροποποιεί τις οδηγίες του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και τις οδηγίες 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 καταργεί την απόφαση 87/95/ΕΟΚ του Συμβουλίου και την απόφαση αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[6]

(33) Η Επιτροπή πρέπει να αναθεωρεί περιοδικά την παρούσα οδηγία, ιδίως προκειμένου να καθορίζεται η ανάγκη τροποποίησης υπό το πρίσμα των μεταβαλλόμενων συνθηκών στην τεχνολογία ή τις αγορές.

(34) Προκειμένου να καταστεί δυνατή η εύρυθμη λειτουργία του δικτύου συνεργασίας, η εξουσία έκδοσης πράξεων σύμφωνα με το άρθρο 290 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης πρέπει να ανατεθεί στην Επιτροπή όσον αφορά τον καθορισμό των κριτηρίων που πρέπει να πληροί ένα κράτος μέλος ώστε να του επιτραπεί να συμμετάσχει στο ασφαλές σύστημα ανταλλαγής πληροφοριών, την περαιτέρω εξειδίκευση των συμβάντων ενεργοποίησης της έγκαιρης προειδοποίησης, καθώς και όσον αφορά τον καθορισμό των περιστάσεων υπό τις οποίες οι φορείς της αγοράς και η δημόσια διοίκηση υποχρεούνται να κοινοποιούν τα συμβάντα.

(35) Έχει ιδιαίτερη σημασία η Επιτροπή να προβαίνει σε κατάλληλες διαβουλεύσεις κατά τη διάρκεια του προπαρασκευαστικού έργου της, μεταξύ άλλων, σε επίπεδο εμπειρογνωμόνων. Η Επιτροπή, όταν ετοιμάζει και συντάσσει κατ' εξουσιοδότηση πράξεις, θα πρέπει να εξασφαλίζει την ταυτόχρονη, έγκαιρη και κατάλληλη διαβίβαση των σχετικών εγγράφων στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.

(36) Προκειμένου να διασφαλιστούν ομοιόμορφοι όροι για την εφαρμογή της παρούσας οδηγίας, πρέπει να ανατεθούν εκτελεστικές εξουσίες στην Επιτροπή όσον αφορά τη συνεργασία μεταξύ των αρμόδιων αρχών και της Επιτροπής εντός του δικτύου συνεργασίας, την πρόσβαση στην υποδομή ασφαλούς ανταλλαγής πληροφοριών, το ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ, τους μορφότυπους και τις διαδικασίες που ισχύουν για την ενημέρωση του κοινού σχετικά με συμβάντα, καθώς και τα πρότυπα ή/και τις τεχνικές προδιαγραφές σχετικά με την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ). Οι αρμοδιότητες αυτές πρέπει να ασκούνται σύμφωνα με τον κανονισμό (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[7].

(37) Κατά την εφαρμογή της παρούσας οδηγίας, η Επιτροπή πρέπει να πραγματοποιεί τις κατάλληλες επαφές με τις σχετικές τομεακές επιτροπές και φορείς σε επίπεδο ΕΕ, ιδίως στους τομείς της ενέργειας, των μεταφορών και της υγείας.

(38) Πληροφορίες που κρίνονται εμπιστευτικές από μια αρμόδια αρχή, σύμφωνα με τους ενωσιακούς και εθνικούς κανόνες περί επιχειρηματικού απορρήτου, πρέπει να ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές μόνον εφόσον η

[6] ΕΕ L 316 της 14.11.2012, σ. 12.
[7] ΕΕ L 55 της 28.2.2011, σ. 13.

ανταλλαγή αυτή είναι απολύτως αναγκαία για την εφαρμογή της παρούσας οδηγίας. Οι κοινοποιούμενες πληροφορίες πρέπει να περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς τους σκοπούς της εν λόγω κοινοποίησης.

(39) Για την ανταλλαγή πληροφοριών σχετικά με κινδύνους και συμβάντα εντός του δικτύου συνεργασίας και για τη συμμόρφωση με τις απαιτήσεις για την κοινοποίηση συμβάντων στις εθνικές αρμόδιες αρχές ενδέχεται να απαιτηθεί επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η εν λόγω επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία για την επίτευξη των στόχων δημοσίου συμφέροντος που επιδιώκονται με την παρούσα οδηγία και, κατά συνέπεια, είναι δικαιολογημένη σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ. Δεν αποτελεί - σε σχέση με τους εν λόγω θεμιτούς σκοπούς - υπέρμετρη και απαράδεκτη παρέμβαση που θίγει αυτή καθεαυτήν την ουσία του δικαιώματος για προστασία των προσωπικών δεδομένων που διασφαλίζεται με το άρθρο 8 του Χάρτη των θεμελιωδών δικαιωμάτων. Κατά την εφαρμογή της παρούσας οδηγίας, ο κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 30ής Μαΐου 2001 για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής[8] εφαρμόζεται ανάλογα με την περίπτωση. Όταν τα δεδομένα υποβάλλονται σε επεξεργασία από τα όργανα και τους οργανισμούς της Ένωσης, η επεξεργασία αυτή προς τον σκοπό εφαρμογής της παρούσας οδηγίας πρέπει να συμμορφώνεται με τον κανονισμό (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών.

(40) Δεδομένου ότι ο στόχος της παρούσας οδηγίας, ήτοι η διασφάλιση υψηλού επιπέδου ΑΔΠ στην Ένωση, είναι αδύνατον να επιτευχθεί επαρκώς αποκλειστικά από τα κράτη μέλη και, συνεπώς, λόγω της κλίμακας ή των αποτελεσμάτων της προβλεπόμενης δράσης, δύναται να επιτευχθεί καλύτερα σε ενωσιακό επίπεδο, η Ένωση μπορεί να θεσπίσει μέτρα, σύμφωνα με την αρχή της επικουρικότητας, όπως ορίζει το άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Σύμφωνα με την αρχή της αναλογικότητας του ίδιου άρθρου, η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη των στόχων αυτών.

(41) Η παρούσα οδηγία σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, και ιδίως το δικαίωμα στο σεβασμό της ιδιωτικής ζωής και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία του επιχειρείν, το δικαίωμα ιδιοκτησίας, το δικαίωμα αποτελεσματικής ένδικης προστασίας ενώπιον δικαστηρίου και το δικαίωμα ακρόασης. Η οδηγία πρέπει να εφαρμόζεται σύμφωνα με τα εν λόγω δικαιώματα και αρχές.

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

ΚΕΦΑΛΑΙΟ Ι

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

[8] ΕΕ L 145 της 31.05.2001, σ. 43.

1. Η παρούσα οδηγία θεσπίζει μέτρα για τη διασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών («εφεξής NIS») εντός της Ένωσης.

2. Για τον σκοπό αυτό, η οδηγία:

α) καθορίζει υποχρεώσεις για όλα τα κράτη μέλη όσον αφορά την πρόληψη, τον χειρισμό και την απόκριση σε κινδύνους και συμβάντα που επηρεάζουν τα συστήματα δικτύων και πληροφοριών ·

β) δημιουργεί ένα μηχανισμό συνεργασίας μεταξύ των κρατών μελών, προκειμένου να διασφαλιστεί ενιαία εφαρμογή της παρούσας οδηγίας εντός της Ένωσης και, εφόσον απαιτηθεί, συντονισμένος και αποτελεσματικός χειρισμός και απόκριση σε κινδύνους και συμβάντα που επηρεάζουν τα συστήματα δικτύων και πληροφοριών ·

γ) θεσπίζει απαιτήσεις ασφάλειας για τους φορείς της αγοράς και για τη δημόσια διοίκηση.

3. Οι απαιτήσεις ασφάλειας που προβλέπονται στο άρθρο 14 δεν εφαρμόζονται στις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών, κατά την έννοια της οδηγίας 2002/21/ΕΚ, οι οποίες πληρούν τις ειδικές απαιτήσεις ασφάλειας και ακεραιότητας που καθορίζονται στα άρθρα 13α και 13β της εν λόγω οδηγίας, ούτε σε παρόχους υπηρεσιών εμπιστοσύνης.

4. Η παρούσα οδηγία δεν θίγει τη νομοθεσία της ΕΕ για το ηλεκτρονικό έγκλημα και την οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την αξιολόγηση της ανάγκης για βελτίωση της προστασίας τους[9].

5. Η παρούσα οδηγία δεν θίγει επίσης την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών[10] και την οδηγία (ΕΚ) αριθ. 2002/58 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, καθώς και τον κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών[11].

6. Για την ανταλλαγή πληροφοριών εντός του δικτύου συνεργασίας σύμφωνα με το κεφάλαιο ΙΙΙ, καθώς και οι ανακοινώσεις συμβάντων ΑΔΠ βάσει του άρθρου 14, ενδέχεται να απαιτηθεί επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η εν λόγω επεξεργασία, απαραίτητη για την επίτευξη των στόχων δημοσίου συμφέροντος που επιδιώκονται με την παρούσα οδηγία, εγκρίνεται από το κράτος μέλος κατ'εφαρμογή του άρθρου 7 της οδηγίας 95/46/ΕΚ και της οδηγίας 2002/58/ΕΚ, όπως έχουν μεταφερθεί στην εθνική νομοθεσία.

Άρθρο 2

Ελάχιστη εναρμόνιση

[9] ΕΕ L 345 της 23.12.2008, σ. 75.
[10] ΕΕ L 281 της 23.11.1995, σ. 31.
[11] SEC(2012) 72 τελικό.

Τα κράτη μέλη δεν εμποδίζονται να θεσπίζουν ή να διατηρούν διατάξεις με τις οποίες εξασφαλίζεται υψηλότερο επίπεδο ασφάλειας, με την επιφύλαξη των υποχρεώσεων που υπέχουν βάσει του ενωσιακού δικαίου.

Άρθρο 3

Ορισμοί

Για τον σκοπό της παρούσας οδηγίας, ισχύουν οι ακόλουθοι ορισμοί:

(1) «σύστημα δικτύων και πληροφοριών»:

α) δίκτυο ηλεκτρονικών επικοινωνιών κατά την έννοια της οδηγίας 2002/21/ΕΚ, και

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών συσκευών, μία ή περισσότερες από τις οποίες, σύμφωνα με πρόγραμμα λογισμικού, εκτελούν αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και

γ) ηλεκτρονικά δεδομένα αποθηκευμένα, επεξεργασμένα, ανακτημένα ή μεταδιδόμενα μέσω των στοιχείων του σημείου (α) και (β) παραπάνω για τους σκοπούς της λειτουργία, χρήσης, προστασίας και συντήρησής τους.

(2) «ασφάλεια»: η ικανότητα ενός συστήματος δικτύων και πληροφοριών να ανθίσταται, με δεδομένο επίπεδο εμπιστοσύνης, σε ατυχήματα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή μεταδιδόμενων δεδομένων ή και τις συναφείς υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω του εν λόγω συστήματος δικτύων και πληροφοριών·

(3) «κίνδυνος»: κάθε περίσταση ή συμβάν που είναι δυνατόν να έχει δυσμενή επίπτωση στην ασφάλεια ·

(4) «συμβάν»: οποιαδήποτε περίσταση ή γεγονός με συγκεκριμένη δυσμενή επίδραση στην ασφάλεια ·

(5) «υπηρεσία της κοινωνίας της πληροφορίας»: υπηρεσία κατά την έννοια του σημείου 2 του άρθρου 1 της οδηγίας 98/34/ΕΚ ·

(6) «σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS)»: σχέδιο στο οποίο καθορίζεται το πλαίσιο των οργανωτικών ρόλων, αρμοδιοτήτων και διαδικασιών για τη διατήρηση ή την αποκατάσταση της λειτουργίας δικτύων και συστημάτων πληροφοριών, σε περίπτωση κινδύνου ή συμβάντος που τα επηρεάζουν

(7) «χειρισμός συμβάντων»: το σύνολο των διαδικασιών που υποστηρίζουν την ανάλυση, τη συγκράτηση και την απόκριση σε συμβάν·

(8) «φορέας της αγοράς»:

α) φορέας παροχής υπηρεσιών της κοινωνίας της πληροφορίας που καθιστά εφικτή την παροχή άλλων υπηρεσιών της κοινωνίας της πληροφορίας, μη εξαντλητικός κατάλογος των οποίων παρατίθεται στο παράρτημα ΙΙ ·

β) φορέας εκμετάλλευσης υποδομών ζωτικής σημασίας, απαραίτητων για τη διατήρηση ζωτικών οικονομικών και κοινωνικών δραστηριοτήτων στα πεδία της ενέργειας, των μεταφορών, των τραπεζών, των χρηματιστηρίων και της υγείας, μη εξαντλητικός κατάλογος των οποίων παρατίθεται στο παράρτημα ΙΙ.

(9) «πρότυπο»: το πρότυπο που προβλέπεται στον κανονισμό (ΕΕ) αριθ. 1025/2012 ·

(10) «προδιαγραφή»: η προδιαγραφή που προβλέπεται στον κανονισμό (ΕΕ) αριθ. 1025/2012 ·

(11) «πάροχος υπηρεσιών εμπιστοσύνης»: φυσικό ή νομικό πρόσωπο που παρέχει κάθε ηλεκτρονική υπηρεσία που συνίσταται στη δημιουργία, επαλήθευση, επικύρωση, διαχείριση και διαφύλαξη ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων, ηλεκτρονικών χρονοσημάνσεων, ηλεκτρονικών εγγράφων, υπηρεσιών ηλεκτρονικής παράδοσης, του ελέγχου γνησιότητας ιστοτόπων και ηλεκτρονικών πιστοποιητικών, συμπεριλαμβανομένων των πιστοποιητικών για ηλεκτρονικές υπογραφές και ηλεκτρονικές σφραγίδες·

ΚΕΦΑΛΑΙΟ ΙΙ

ΕΘΝΙΚΑ ΠΛΑΙΣΙΑ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 4

Αρχή

Τα κράτη μέλη διασφαλίζουν υψηλό επίπεδο ασφάλειας των συστημάτων δικτύων και πληροφοριών στην επικράτειά τους σύμφωνα με την παρούσα οδηγία.

Άρθρο 5

Εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ) και εθνικό σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών

(1) Κάθε κράτος μέλος θεσπίζει εθνική στρατηγική ΑΔΠ που καθορίζει τους στρατηγικούς στόχους και συγκεκριμένα μέτρα, πολιτικής και ρυθμιστικά, για να επιτευχθεί και να διατηρηθεί υψηλό επίπεδο ασφάλειας δικτύων και πληροφοριών. Η εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών αφορά ιδίως τα ακόλουθα θέματα:

α) τον ορισμό των στόχων και των προτεραιοτήτων της στρατηγικής, με βάση επικαιροποιημένη ανάλυση κινδύνου και συμβάντων ·

β) το πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της στρατηγικής, συμπεριλαμβανομένου σαφούς ορισμού των ρόλων και αρμοδιοτήτων των κυβερνητικών φορέων και των λοιπών σχετικών φορέων ·

γ) προσδιορισμό των γενικών μέτρων ετοιμότητας, απόκρισης και αποκατάστασης, συμπεριλαμβανομένων των μηχανισμών συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα ·

δ) Ενδεικτική αναφορά στα προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης ·

ε) ερευνητικά και αναπτυξιακά σχέδια και περιγραφή του τρόπου με τον οποίο τα σχέδια αυτά αντανακλούν τις προτεραιότητες που έχουν καθοριστεί.

(2) Η εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών περιλαμβάνει ένα εθνικό σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών που συμμορφώνεται τουλάχιστον με τις ακόλουθες απαιτήσεις:

α) σχέδιο εκτίμησης του κινδύνου για να προσδιοριστούν κίνδυνοι και να εκτιμηθεί ο αντίκτυπος ενδεχόμενων συμβάντων ·

β) με τον καθορισμό των ρόλων και αρμοδιοτήτων των διαφόρων συντελεστών που εμπλέκονται στην υλοποίηση του σχεδίου·

γ) με τον καθορισμό των διαδικασιών συνεργασίας και επικοινωνίας για την εξασφάλιση πρόληψης, ανίχνευσης, απόκρισης, αποκατάστασης και ανάκτησης, προσαρμοσμένων ανάλογα με το επίπεδο συναγερμού ·

δ) με την πρόβλεψη για χάρτη πορείας για ασκήσεις και κατάρτιση σε ΑΔΠ με σκοπό να ενισχυθεί, να επικυρωθεί και να δοκιμαστεί το σχέδιο. τυχόν διδάγματα πρέπει να τεκμηριώνονται και να εντάσσονται σε επικαιροποιήσεις του σχεδίου.

(3) Η εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών και το εθνικό σχέδιο συνεργασίας για την ΑΔΠ κοινοποιούνται στην Επιτροπή εντός ενός μηνός από την έγκρισή τους.

Άρθρο 6

Αρμόδια εθνική αρχή για την ασφάλεια των συστημάτων δικτύων και πληροφοριών

1. Κάθε κράτος μέλος ορίζει μια εθνική αρμόδια αρχή σχετικά με την ασφάλεια των συστημάτων δικτύων και πληροφοριών (στο εξής «η αρμόδια αρχή»).

2. Οι αρμόδιες αρχές παρακολουθούν την εφαρμογή της παρούσας οδηγίας σε εθνικό επίπεδο και συμβάλλουν στη συνεκτική εφαρμογή της σε όλη την Ένωση.

3. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν επαρκείς τεχνικούς, οικονομικούς και ανθρώπινους πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντα που τους έχουν ανατεθεί και, με τον τρόπο αυτό, ότι επιτυγχάνουν τους στόχους της παρούσας οδηγίας. Τα κράτη μέλη μεριμνούν για την αποτελεσματική, αποδοτική και ασφαλή συνεργασία των αρμόδιων αρχών μέσω του δικτύου που αναφέρεται στο άρθρο 8.

4. Τα κράτη μέλη διασφαλίζουν ότι οι αρμόδιες αρχές λαμβάνουν τις κοινοποιήσεις των συμβάντων από τη δημόσια διοίκηση και τους φορείς της αγοράς όπως ορίζεται από το άρθρο 14 παράγραφος 2 και ότι τους ανατίθενται οι αρμοδιότητες εφαρμογής και επιβολής που αναφέρονται στο άρθρο 15.

5. Οι αρμόδιες αρχές πραγματοποιούν διαβουλεύσεις και συνεργάζονται, κατά περίπτωση, με τις σχετικές εθνικές αρχές επιβολής του νόμου και με τις αρχές προστασίας των δεδομένων.

6. Κάθε κράτος μέλος κοινοποιεί στην Επιτροπή, χωρίς καθυστέρηση, τον διορισμό της αρμόδιας αρχής και τα καθήκοντά της, καθώς και κάθε μεταγενέστερη σχετική τροποποίηση. Κάθε κράτος μέλος δημοσιεύει τον διορισμό της αρμόδιας αρχής.

Άρθρο 7

Ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική

1. Κάθε κράτος μέλος καταρτίζει κατάσταση Ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (εφεξής: «CERT») που είναι υπεύθυνη για τον χειρισμό συμβάντων και κινδύνων σύμφωνα με επακριβώς καθορισμένη διαδικασία, η οποία πρέπει να συμμορφώνεται με τις απαιτήσεις που αναφέρονται στο σημείο (1) του παραρτήματος Ι. Η CERT μπορεί να ιδρυθεί εντός της αρμόδιας αρχής.

2. Τα κράτη μέλη εξασφαλίζουν ότι οι ομάδες CERT διαθέτουν επαρκείς τεχνικούς, οικονομικούς και ανθρώπινους πόρους για την αποτελεσματική εκτέλεση των εργασιών που περιγράφονται στο σημείο 2 του παραρτήματος Ι.

3. Τα κράτη μέλη εξασφαλίζουν ότι οι ομάδες CERT βασίζονται σε ασφαλή και ανθεκτική υποδομή επικοινωνιών και πληροφοριών σε εθνικό επίπεδο, συμβατή και διαλειτουργική με το ασφαλές σύστημα ανταλλαγής πληροφοριών που αναφέρεται στο άρθρο 9.

4. Τα κράτη μέλη ενημερώνουν την Επιτροπή σχετικά με τους πόρους και την εντολή, καθώς και με τη διαδικασία αντιμετώπισης συμβάντων των ομάδων CERT.

5. Η CERT ενεργεί υπό την εποπτεία της αρμόδιας αρχής, η οποία επανεξετάζει σε τακτά διαστήματα την επάρκεια των πόρων που διαθέτει, την αποστολή και την αποτελεσματικότητα της διαδικασίας χειρισμού συμβάντων.

ΚΕΦΑΛΑΙΟ ΙΙΙ

ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΑΡΜΟΔΙΩΝ ΑΡΧΩΝ

Άρθρο 8

Δίκτυο συνεργασίας

1. Οι αρμόδιες αρχές και η Επιτροπή συγκροτούν δίκτυο («δίκτυο συνεργασίας») που συνεργάζεται για την αντιμετώπιση κινδύνων και συμβάντων που επηρεάζουν τα συστήματα δικτύων και πληροφοριών.

2. Στο πλαίσιο του δικτύου συνεργασίας βρίσκονται σε συνεχή επικοινωνία η Επιτροπή με τις αρμόδιες αρχές. Εφόσον ζητηθεί, ο ευρωπαϊκός οργανισμός ασφάλειας δικτύων και πληροφοριών («ENISA») επικουρεί το δίκτυο συνεργασίας παρέχοντας την εμπειρογνωμοσύνη και τις συμβουλές του.

3. Εντός του δικτύου συνεργασίας οι αρμόδιες αρχές:

α) διαβιβάζουν έγκαιρες προειδοποιήσεις σχετικά με κινδύνους και συμβάντα σύμφωνα με το άρθρο 10 ·

β) εξασφαλίζουν συντονισμένη απόκριση σύμφωνα με το άρθρο 11 ·

γ) δημοσιεύουν σε τακτική βάση σε κοινό ιστότοπο τις μη εμπιστευτικές πληροφορίες σχετικά με τις εν εξελίξει έγκαιρες προειδοποιήσεις και τη συντονισμένη απόκριση·

δ) εξετάζουν και αξιολογούν από κοινού, κατόπιν αιτήματος ενός κράτους μέλους ή της Επιτροπής, μία ή περισσότερες εθνικές στρατηγικές ΑΔΠ και εθνικά σχέδια συνεργασίας ΑΔΠ που αναφέρονται στο άρθρο 5, εντός του πεδίου εφαρμογής της παρούσας οδηγίας.

ε) εξετάζουν και αξιολογούν από κοινού, έπειτα από αίτηση κράτους μέλους ή της Επιτροπής, την αποτελεσματικότητα των CERT, ιδίως όταν πραγματοποιούνται ασκήσεις σχετικά με την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ) σε επίπεδο Ένωσης·

στ) συνεργάζονται και ανταλλάσσουν πληροφορίες για όλα τα συναφή θέματα με το ευρωπαϊκό κέντρο ηλεκτρονικού εγκλήματος της Ευρωπόλ, καθώς και με άλλους συναφείς ευρωπαϊκούς οργανισμούς, ιδίως στα πεδία της προστασίας των δεδομένων, της ενέργειας, των μεταφορών, των τραπεζών, των χρηματιστηρίων και της υγείας ·

ζ) ανταλλάσσουν πληροφορίες και βέλτιστη πρακτική μεταξύ των ιδίων και της Επιτροπής, και αλληλοβοηθούνται στην ανάπτυξη ικανοτήτων σχετικά με την ασφάλεια δικτύων και πληροφοριών ·

η) διοργανώνουν τακτικές αξιολογήσεις από ομοτίμους σχετικά με τις ικανότητες και την ετοιμότητά τους ·

θ) διοργανώνουν σε ενωσιακό επίπεδο ασκήσεις σχετικά με την ασφάλεια δικτύων και πληροφοριών και, κατά περίπτωση, συμμετέχουν σε διεθνείς ασκήσεις σχετικά με την ασφάλεια δικτύων και πληροφοριών.

4. Η Επιτροπή θεσπίζει, με εκτελεστικές πράξεις, τις αναγκαίες λεπτομέρειες για τη διευκόλυνση της συνεργασίας μεταξύ αρμόδιων αρχών και της Επιτροπής που αναφέρεται στις παραγράφους 2 και 3. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία διαβούλευσης του άρθρου 19 παράγραφος 2.

Άρθρο 9

Ασφαλές σύστημα ανταλλαγής πληροφοριών

1. Η ανταλλαγή ευαίσθητων και εμπιστευτικών πληροφοριών εντός του δικτύου συνεργασίας εκτελείται μέσω ασφαλούς υποδομής.

2. Ανατίθεται στην Επιτροπή η έκδοση κατ'εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 18 σχετικά με τον ορισμό των κριτηρίων που πρέπει να πληρούνται από ένα κράτος μέλος ώστε να επιτρέπεται η συμμετοχή του στο ασφαλές σύστημα ανταλλαγής πληροφοριών, όσον αφορά:

α) τη διαθεσιμότητα ασφαλούς και ανθεκτικής υποδομής επικοινωνιών και πληροφοριών σε εθνικό επίπεδο, συμβατής και διαλειτουργικής με την ασφαλή υποδομή του δικτύου συνεργασίας σύμφωνα με το άρθρο 7, παράγραφος 3, και

β) την ύπαρξη επαρκών τεχνικών, χρηματοδοτικών και ανθρώπινων πόρων και διαδικασιών ώστε η αρμόδια αρχή τους και η CERT να έχει τη δυνατότητα αποτελεσματικής, αποδοτικής και ασφαλούς συμμετοχής στο ασφαλές σύστημα ανταλλαγής πληροφοριών βάσει του άρθρου 6 παράγραφος 3, του άρθρου 7 παράγραφος 2 και του άρθρου 7 παράγραφος 3.

3. Μέσω εκτελεστικών πράξεων, η Επιτροπή θεσπίζει αποφάσεις σχετικά με την πρόσβαση των κρατών μελών στην εν λόγω υποδομή, σύμφωνα με τα κριτήρια που αναφέρονται στην παράγραφο 2 και 3. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 19 παράγραφος 3.

Άρθρο 10

Έγκαιρες προειδοποιήσεις

1. Οι αρμόδιες αρχές ή η Επιτροπή παρέχουν έγκαιρες προειδοποιήσεις εντός του δικτύου συνεργασίας σχετικά με εκείνους τους κινδύνους και τα συμβάντα που πληρούν τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) αυξάνονται ταχέως ή μπορεί να αυξάνονται ταχέως σε κλίμακα ·

β) υπερβαίνουν ή μπορούν να υπερβούν την εθνική ικανότητα απόκρισης ·

γ) επηρεάζουν ή ενδέχεται να επηρεάσουν, περισσότερα από ένα κράτη μέλη.

2. Στην έγκαιρη προειδοποίηση, οι αρμόδιες αρχές και η Επιτροπή γνωστοποιούν κάθε σχετική πληροφορία που έχουν στη διάθεσή τους, που μπορεί να είναι χρήσιμη για την αξιολόγηση του κινδύνου ή του συμβάντος.

3. Έπειτα από αίτηση κράτους μέλους, ή με δική της πρωτοβουλία, η Επιτροπή μπορεί να ζητήσει από το κράτος μέλος να υποβάλει κάθε σχετική πληροφορία σχετικά με συγκεκριμένο κίνδυνο ή συμβάν.

4. Σε περίπτωση που για κίνδυνο ή συμβάν που είναι αντικείμενο έγκαιρης προειδοποίησης υφίσταται υποψία ποινικού χαρακτήρα, οι αρμόδιες αρχές ή η Επιτροπή ενημερώνουν το ευρωπαϊκό κέντρο ηλεκτρονικού εγκλήματος της Ευρωπόλ.

5. Παρέχεται στην Επιτροπή η εξουσία έκδοσης κατ'εξουσιοδότηση πράξεων σύμφωνα με το άρθρο 18, το οποίο αφορά τον περαιτέρω προσδιορισμό των κινδύνων και συμβάντων που ενεργοποιούν έκδοση έγκαιρης προειδοποίησης της παραγράφου 1.

Άρθρο 11

Συντονισμένη απόκριση

1. Έπειτα από έγκαιρη προειδοποίηση του άρθρου 10, οι αρμόδιες αρχές, αφού αξιολογήσουν τις σχετικές πληροφορίες, συμφωνούν για μια συντονισμένη απόκριση σύμφωνα με το ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ που αναφέρεται στο άρθρο 12.

2. Τα διάφορα μέτρα που θεσπίζονται σε εθνικό επίπεδο ως αποτέλεσμα της συντονισμένης απόκρισης ανακοινώνεται στο δίκτυο συνεργασίας.

Άρθρο 12

Ενωσιακό σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών

1. Η Επιτροπή εξουσιοδοτείται να εγκρίνει, με εκτελεστικές πράξεις, ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 19 παράγραφος 3.

2. Το ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ προβλέπει:

α) για τους σκοπούς του άρθρου 10:

– καθορισμό του μορφότυπου και των διαδικασιών για τη συλλογή και την ανταλλαγή, από τις αρμόδιες αρχές, συμβατών και συγκρίσιμων πληροφοριών σχετικά με κινδύνους και συμβάντα,

– καθορισμό των διαδικασιών και των κριτηρίων για την αξιολόγηση, από το δίκτυο συνεργασίας, των κινδύνων και συμβάντων.

β) τις ακολουθητέες διαδικασίες για τις συντονισμένες απαντήσεις βάσει του άρθρου 11, συμπεριλαμβανομένου του προσδιορισμού ρόλων και αρμοδιοτήτων, καθώς και διαδικασιών συνεργασίας ·

γ) χάρτη πορείας για ασκήσεις και κατάρτιση σε ΑΔΠ με σκοπό να ενισχυθεί, επικυρωθεί και δοκιμαστεί το σχέδιο·

δ) πρόγραμμα για μεταφορά γνώσεων μεταξύ των κρατών μελών όσον αφορά την ανάπτυξη ικανοτήτων και τη μάθηση μέσω ομοτίμων·

ε) πρόγραμμα ευαισθητοποίησης και κατάρτισης μεταξύ των κρατών μελών.

3. Το ενωσιακό σχέδιο συνεργασίας για την ΑΔΠ εγκρίνεται το αργότερο ένα έτος ύστερα την έναρξη ισχύος της παρούσας οδηγίας και αναθεωρείται τακτικά.

Άρθρο 13

Διεθνής συνεργασία

Με την επιφύλαξη της δυνατότητας για το δίκτυο συνεργασίας να έχει άτυπη διεθνή συνεργασία, η Ένωση μπορεί να συνάπτει διεθνείς συμφωνίες με τρίτες χώρες ή διεθνείς οργανισμούς που επιτρέπει και οργανώνει τη συμμετοχή τους σε ορισμένες δραστηριότητες του δικτύου συνεργασίας. Η εν λόγω συμφωνία λαμβάνει υπόψη την ανάγκη να εξασφαλιστεί επαρκής προστασία των δεδομένων προσωπικού χαρακτήρα που κυκλοφορούν στο δίκτυο συνεργασίας.

ΚΕΦΑΛΑΙΟ IV

ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΟΥΣ ΦΟΡΕΙΣ ΤΗΣ ΑΓΟΡΑΣ

Άρθρο 14

Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων

1. Τα κράτη μέλη εξασφαλίζουν ότι η δημόσια διοίκηση και οι φορείς της αγοράς λαμβάνουν κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που ελέγχουν και χρησιμοποιούν στην επιχειρησιακή λειτουργία τους. Λαμβανομένων υπόψη των πλέον πρόσφατων τεχνικών δυνατοτήτων, τα μέτρα αυτά εγγυώνται επίπεδο ασφάλειας ανάλογο προς τους παρουσιαζόμενους κινδύνους. Ιδιαιτέρως, λαμβάνονται μέτρα για την αποτροπή και ελαχιστοποίηση του αντίκτυπου από συμβάντα που επηρεάζουν το οικείο δίκτυο και σύστημα πληροφοριών ως προς τις βασικές υπηρεσίες που παρέχουν, εξασφαλίζοντας επομένως τη συνέχεια της παροχής υπηρεσιών που στηρίζονται σε αυτά τα δίκτυα και τα συστήματα πληροφοριών.

2. Τα κράτη μέλη εξασφαλίζουν ότι οι δημόσιες διοικήσεις και οι φορείς της αγοράς κοινοποιούν στην αρμόδια αρχή συμβάντα με σημαντικό αντίκτυπο στην ασφάλεια των βασικών υπηρεσιών που παρέχουν.

3. Οι απαιτήσεις των παραγράφων 1 και 2 ισχύουν για όλους τους φορείς της αγοράς που παρέχουν υπηρεσίες εντός της Ευρωπαϊκής Ένωσης.

4. Η αρμόδια αρχή μπορεί να ενημερώσει το κοινό ή να απαιτήσει από τη δημόσια διοίκηση και τους φορείς της αγοράς να το πράξουν, εφόσον κρίνει ότι η αποκάλυψη του συμβάντος είναι προς το δημόσιο συμφέρον. Η εθνική ρυθμιστική αρχή υποβάλει μία φορά ετησίως στο δίκτυο συνεργασίας συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και την δράση που έχει αναλάβει σύμφωνα με την παρούσα παράγραφο.

5. Η Επιτροπή εξουσιοδοτείται να εγκρίνει κατ’εξουσιοδότηση πράξεις σύμφωνα με το άρθρο 18 για τον ορισμό των περιστάσεων κατά τις οποίες η δημόσια διοίκηση και οι φορείς της αγοράς είναι υποχρεωμένοι να κοινοποιούν συμβάντα.

6. Με την επιφύλαξη τυχόν κατ’εξουσιοδότηση πράξεων που έχουν εγκριθεί σύμφωνα με την παράγραφο 5, οι αρμόδιες αρχές μπορούν να εκδίδουν κατευθυντήριες γραμμές και, εφόσον είναι αναγκαίο, να δίδουν οδηγίες σχετικά με τις περιστάσεις

υπό τις οποίες η δημόσια διοίκηση και οι φορείς της αγοράς είναι υποχρεωμένοι να κοινοποιούν συμβάντα.

7. Η Επιτροπή εξουσιοδοτείται να καθορίζει, μέσω εκτελεστικών πράξεων, τους μορφότυπους και τις διαδικασίες που εφαρμόζονται για τους σκοπούς της παραγράφου 2. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης στην οποία παραπέμπει το άρθρο 19 παράγραφος 3.

8. Οι παράγραφοι 1 και 2 δεν εφαρμόζονται στις πολύ μικρές επιχειρήσεις, όπως ορίζεται στη σύσταση 2003/361/ΕΚ της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων[12].

Άρθρο 15

Εφαρμογή και επιβολή

1. Τα κράτη μέλη μεριμνούν ώστε οι αρμόδιες αρχές να διαθέτουν όλες τις απαραίτητες εξουσίες για τη διερεύνηση περιπτώσεων μη συμμόρφωσης, της δημόσιας διοίκησης ή φορέων της αγοράς, με τις υποχρεώσεις που υπέχουν βάσει του άρθρου 14 και των επιπτώσεών τους στην ασφάλεια των δικτύων και των συστημάτων πληροφοριών.

2. Τα κράτη μέλη εξασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία να ζητούν από τους φορείς της αγοράς και τη δημόσια διοίκηση:

   α) να παρέχουν πληροφορίες απαραίτητες για την εκτίμηση της ασφάλειας των δικτύων και των υπηρεσιών πληροφοριών τους, συμπεριλαμβανομένων τεκμηριωμένων πολιτικών ασφάλειας·

   β) να υποβάλλονται σε έλεγχο ασφάλειας που διενεργείται από ειδικευμένο ανεξάρτητο φορέα ή εθνική αρχή και να θέτουν τα σχετικά πορίσματα στη διάθεση της αρμόδιας αρχής.

3. Τα κράτη μέλη εξασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν την εξουσία έκδοσης δεσμευτικών οδηγιών προς τους φορείς της αγοράς και τη δημόσια διοίκηση.

4. Οι αρμόδιες αρχές κοινοποιούν στις αρχές επιβολής του νόμου συμβάντα όπου υπάρχει υπόνοια σοβαρού ποινικού χαρακτήρα.

5. Κατά την αντιμετώπιση συμβάντων παραβίασης προσωπικών δεδομένων οι αρμόδιες αρχές συνεργάζονται στενά με τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα.

6. Τα κράτη μέλη εξασφαλίζουν ότι τυχόν υποχρεώσεις που επιβάλλονται στη δημόσια διοίκηση και τους φορείς της αγοράς δυνάμει του παρόντος κεφαλαίου μπορεί να υπόκεινται σε δικαστικό έλεγχο.

Άρθρο 16

Τυποποίηση

1. Για να εξασφαλιστεί συγκλίνουσα εφαρμογή του άρθρου 14 παράγραφος 1, τα κράτη μέλη ενθαρρύνουν τη χρήση των προτύπων ή/και προδιαγραφών σχετικών με την ασφάλεια δικτύων και πληροφοριών.

[12] ΕΕ L 124 της 20.05.2003, σ. 36.

2. Η Επιτροπή καταρτίζει, *με εκτελεστικές πράξεις,* κατάλογο των προτύπων που αναφέρονται στην παράγραφο 1. Ο κατάλογος δημοσιεύεται στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης .

ΚΕΦΑΛΑΙΟ V

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ.

Άρθρο 17

Κυρώσεις

1. Τα κράτη μέλη καθορίζουν τους κανόνες για τις επιβλητέες κυρώσεις σε περίπτωση παραβίασης 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 πρέπει να είναι ουσιαστικές, αναλογικές και αποτρεπτικές. Τα κράτη μέλη κοινοποιούν τις εν λόγω διατάξεις στην Επιτροπή, το αργότερο κατά την ημερομηνία μεταφοράς της παρούσας οδηγίας, κοινοποιούν δε χωρίς καθυστέρηση κάθε επακόλουθη τροποποίηση που τις επηρεάζει.

2. Τα κράτη μέλη εξασφαλίζουν ότι, εφόσον ένα συμβάν ασφάλειας περιλαμβάνει προσωπικά δεδομένα, οι προβλεπόμενες κυρώσεις είναι σύμφωνες με τις κυρώσεις που προβλέπονται από τον κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών[13]

Άρθρο 18

Άσκηση της εξουσιοδότησης

1. Η εξουσία για την έκδοση των κατ' εξουσιοδότηση πράξεων ανατίθεται στην Επιτροπή με την επιφύλαξη των όρων που ορίζονται στο παρόν άρθρο.

2. Η εξουσία έκδοσης κατ'εξουσιοδότηση πράξεων που αναφέρεται στο άρθρο 9 παράγραφος 2, το άρθρο 10 παράγραφος 5 και το άρθρο 14 παράγραφος 5 ανατίθεται στην Επιτροπή. Η Επιτροπή συντάσσει έκθεση σχετικά με την εξουσιοδότηση το αργότερο εννέα μήνες πριν από την εκπνοή της πενταετούς περιόδου. Η εξουσιοδότηση παρατείνεται σιωπηρά για χρονικές περιόδους της ίδιας διάρκειας, εκτός εάν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο αντιτεθούν σε αυτή την παράταση, το αργότερο τρεις μήνες πριν από το τέλος κάθε περιόδου.

3. Η εξουσιοδότηση που προβλέπεται στο άρθρο 9 παράγραφος 2, στο άρθρο 10 παράγραφος 5 και στο άρθρο 14 παράγραφος 5, 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. Παράγει αποτελέσματα από την επομένη της δημοσίευσης της απόφασης στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης* ή σε μεταγενέστερη ημερομηνία που καθορίζεται στην απόφαση. Η απόφαση δεν θίγει την εγκυρότητα καμίας από τις ήδη ισχύουσες κατ' εξουσιοδότηση πράξεις.

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

---

13 SEC(2012) 72 τελικό

5. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει των άρθρων 9 παράγραφος 2, 10 παράγραφος 5 και 14 παράγραφος 5, τίθεται σε ισχύ μόνον εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο εντός δύο μηνών από την ημέρα που η πράξη κοινοποιείται στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ή εάν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλλουν αντιρρήσεις. Η περίοδος αυτή παρατείνεται κατά δύο μήνες κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.

Άρθρο 19

Διαδικασία Επιτροπής

1. Η Ευρωπαϊκή Επιτροπή επικουρείται από επιτροπή (την επιτροπή για την ασφάλεια δικτύων και πληροφοριών). Η εν λόγω επιτροπή είναι επιτροπή κατά την έννοια του κανονισμού (ΕΕ) αριθ. 182/2011.

2. Στις περιπτώσεις που γίνεται μνεία της παρούσας παραγράφου, εφαρμόζεται το άρθρο 4 του κανονισμού (ΕΕ) αριθ. 182/2011.

3. Στις περιπτώσεις που γίνεται μνεία της παρούσας παραγράφου, εφαρμόζεται το άρθρο 5 του κανονισμού (ΕΕ) αριθ. 182/2011.

Άρθρο 20

Επανεξέταση

Η Επιτροπή προβαίνει σε περιοδική επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Η πρώτη έκθεση θα υποβληθεί το αργότερο τρία έτη έπειτα από την ημερομηνία μεταφοράς που αναφέρεται στο άρθρο 21. Για το σκοπό αυτό, η Επιτροπή μπορεί να ζητήσει από τα κράτη μέλη να παράσχουν πληροφορίες χωρίς αδικαιολόγητη καθυστέρηση.

Άρθρο 21

Μεταφορά στο εθνικό δίκαιο

1. Τα κράτη μέλη θεσπίζουν και δημοσιεύουν το αργότερο έως τις [18 μήνες έπειτα από την έκδοση της οδηγίας] τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν προς την παρούσα οδηγία. Ανακοινώνουν αμέσως στην Επιτροπή το κείμενο των εν λόγω διατάξεων.

   Εφαρμόζουν τα εν λόγω μέτρα από τις [18 μήνες από την έκδοση της οδηγίας].

   Οι διατάξεις αυτές, όταν θεσπίζονται από τα κράτη μέλη, αναφέρονται στην παρούσα οδηγία ή συνοδεύονται από παρόμοια αναφορά κατά την επίσημη δημοσίευσή τους. Οι λεπτομερείς διατάξεις για την αναφορά αυτή καθορίζονται από τα κράτη μέλη.

2. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή το κείμενο των ουσιωδών διατάξεων εσωτερικού δικαίου τις οποίες θεσπίζουν στον τομέα που διέπεται από την παρούσα οδηγία.

Άρθρο 22

Έναρξη ισχύος

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

Άρθρο 23

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες,

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

ΠΑΡΑΡΤΗΜΑ Ι

Απαιτήσεις και καθήκοντα της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT)

Οι απαιτήσεις και τα καθήκοντα της CERT είναι επαρκώς και σαφώς καθορισμένα και στηρίζονται από εθνική πολιτική ή/και κανονιστική ρύθμιση. Περιλαμβάνουν τα ακόλουθα στοιχεία:

(1) Απαιτήσεις για τη CERT

α) Η CERT εξασφαλίζει ευρεία διαθεσιμότητα των υπηρεσιών επικοινωνιών της αποφεύγοντας μονοσημειακές αστοχίες και προσφέρει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους. Επιπλέον, οι δίαυλοι επικοινωνίας πρέπει να είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στην κοινότητα και στους εταίρους της συνεργασίας.

β) Η CERT εφαρμόζει και διαχειρίζεται μέτρα ασφάλειας για να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα των πληροφοριών που λαμβάνει και χειρίζεται.

γ) Τα γραφεία της CERT και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους.

δ) Συστήνεται σύστημα ποιότητας διαχείρισης υπηρεσιών για την παρακολούθηση των επιδόσεων της CERT και για την εξασφάλιση διαρκούς διαδικασίας βελτίωσης. Βασίζεται σε σαφώς καθορισμένα κριτήρια μέτρησης που περιλαμβάνουν επίσημα επίπεδα παρεχόμενων υπηρεσιών και βασικούς δείκτες επιδόσεων.

ε) Συνέχεια της επιχειρηματικής δραστηριότητας:

– Η CERT είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων,

– Η CERT είναι επαρκώς στελεχωμένη ώστε να εξασφαλίζεται η διαθεσιμότητα ανά πάσα στιγμή,

– Η CERT βασίζεται σε υποδομή, η συνέχεια της οποίας είναι διασφαλισμένη . Για το σκοπό αυτό, συστήνονται πλεονάζοντα συστήματα και εφεδρικές περιοχές εργασίας για τη CERT, ώστε να εξασφαλίζεται διαρκής πρόσβαση στους τρόπους επικοινωνίας.

(2) Καθήκοντα της CERT

α) Στα καθήκοντα της CERT περιλαμβάνουν τουλάχιστον τα εξής:

– Παρακολούθηση συμβάντων σε εθνικό επίπεδο,

– Παροχή έγκαιρης προειδοποίησης, ειδοποιήσεων επαγρύπνησης, ανακοινώσεων και διάδοσης των πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα,

– Απόκριση σε συμβάντα,

– Παροχή δυναμικής ανάλυσης κινδύνου και συμβάντων και επίγνωση της κατάστασης,

– Ανάπτυξη ευρείας ευαισθητοποίησης του κοινού σχετικά με τους κινδύνους που συνδέονται με δραστηριότητες στο διαδίκτυο,

– Διοργάνωση εκστρατειών ευαισθητοποίησης για την ασφάλεια δικτύων και πληροφοριών (NIS) ·

β) Η CERT εγκαθιδρύει σχέσεις συνεργασίας με τον ιδιωτικό τομέα.

γ) Προς διευκόλυνση της συνεργασίας, η CERT προωθεί την υιοθέτηση και χρήση κοινών ή τυποποιημένων πρακτικών για:

– διαδικασίες χειρισμού συμβάντων ή κινδύνου,

– συστήματα ταξινόμησης συμβάντων, κινδύνου και πληροφοριών,

– ταξινομήσεις για συστήματα μέτρησης,

– μορφότυπους ανταλλαγής πληροφοριών σχετικά με κινδύνους, συμβάντα, καθώς και συμβάσεις ονοματοδοσίας συστημάτων.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Κατάλογος των φορέων εκμετάλλευσης της αγοράς

που αναφέρονται στο άρθρο 3 παράγραφος 8 στοιχείο α)

1. πλατφόρμες ηλ-εμπορίου

2. Πύλες πληρωμών μέσω διαδικτύου

3. Κοινωνικά δίκτυα

4. Μηχανές έρευνας

5. Υπηρεσίες υπολογιστικού νέφους

6. Καταστήματα ηλ-εφαρμογών

που αναφέρονται στο άρθρο 3 παράγραφος 8 στοιχείο β)

1. Ενέργεια

- προμηθευτές ηλεκτρικής ενέργειας και φυσικού αερίου
- φορείς εκμετάλλευσης συστημάτων διανομής ηλεκτρικής ενέργειας και εταιρείες λιανικής πώλησης για τους τελικούς καταναλωτές
- φορείς εκμετάλλευσης συστημάτων μεταφοράς φυσικού αερίου, διαχειριστές εγκαταστάσεων αποθήκευσης και LNG (ΥΦΑ)
- φορείς εκμετάλλευσης συστημάτων μεταφοράς ηλεκτρικής ενέργειας
- αγωγοί μεταφοράς πετρελαίου και αποθήκευση πετρελαίου
- φορείς εκμετάλλευσης αγοράς ηλεκτρικής ενέργειας και φυσικού αερίου
- φορείς εκμετάλλευσης πετρελαίου και φυσικού αερίου στην παραγωγή, τη διύλιση και τις εγκαταστάσεις επεξεργασίας

2. Μεταφορές

- αερομεταφορείς (εμπορεύματα και επιβάτες αεροπορικών μεταφορών).
- θαλάσσιοι μεταφορείς (θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εταιρείες θαλάσσιων και ακτοπλοϊκών μεταφορών εμπορευμάτων)
- σιδηρόδρομοι (διαχειριστές υποδομής, καθετοποιημένες εταιρείες και φορείς εκμετάλλευσης σιδηροδρομικών μεταφορών)
- αερολιμένες
- λιμένες
- φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας
- βοηθητικές υπηρεσίες εφοδιαστικής (α) αποθήκευση και αποθεματοποίηση, β) διακίνηση φορτίων και γ) λοιπές υποστηρικτικές δραστηριότητες στις μεταφορές)

3. Τράπεζες: πιστωτικά ιδρύματα σύμφωνα με το άρθρο 4 παρ. 1 της οδηγίας 2006/48/ΕΚ.

4. υποδομές χρηματοπιστωτικών αγορών: χρηματιστήρια και γραφεία συμψηφισμού κεντρικού αντισυμβαλλομένου

5. Τομέας της υγείας: περιβάλλοντα υγειονομικής περίθαλψης (όπως νοσοκομεία και ιδιωτικές κλινικές) και άλλες οντότητες που εμπλέκονται σε διατάξεις υγειονομικής περίθαλψης

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Ονομασία της πρότασης/πρωτοβουλίας

1.2. Σχετικός(οί) τομέας(είς) πολιτικής που αφορά(ούν) τη δομή ΔΒΔ/ΠΒΔ

1.3. Χαρακτήρας της πρότασης/πρωτοβουλίας

1.4. Στόχοι

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.6. Διάρκεια και δημοσιονομικός αντίκτυπος της δράσης

1.7. Προβλεπόμενος(οι) τρόπος(οι) διαχείρισης

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Διατάξεις στον τομέα της παρακολούθησης και της υποβολής εκθέσεων

2.2. Σύστημα διαχείρισης και ελέγχου

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

3. ΕΚΤΙΜΩΜΕΝΟΣ ΔΗΜΟΣΙΟΝΟΜΙΚΟΣ ΑΝΤΙΚΤΥΠΟΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

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

3.2. Εκτιμώμενος αντίκτυπος στις δαπάνες

3.2.1. Συνοπτική παρουσίαση του εκτιμώμενου αντίκτυπου στις δαπάνες

3.2.2. Εκτιμώμενος αντίκτυπος στις επιχειρησιακές πιστώσεις

3.2.3. Εκτιμώμενος αντίκτυπος στις πιστώσεις διοικητικού χαρακτήρα

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

3.2.5. Συμμετοχή τρίτων μερών στη χρηματοδότηση

3.3. Εκτιμώμενος δημοσιονομικός αντίκτυπος στα έσοδα

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Ονομασία της πρότασης/πρωτοβουλίας

Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για την εξασφάλιση υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση.

1.2. Σχετικός(-οί) τομέας(-είς) πολιτικής στη διάρθρωση ΔΒΔ/ΠΒΔ[37]:

09 – δίκτυα, περιεχόμενο και τεχνολογία επικοινωνιών

1.3. Χαρακτήρας της πρότασης/πρωτοβουλίας

☒ Η πρόταση/πρωτοβουλία αφορά **νέα δράση**

☐ Η πρόταση/πρωτοβουλία αφορά **νέα δράση έπειτα από πιλοτικό έργο/προπαρασκευαστική δράση**[38]

☐ Η πρόταση/πρωτοβουλία αφορά **επέκταση υφιστάμενης δράσης**

☐ Η πρόταση/πρωτοβουλία αφορά **δράση αναπροσανατολισμένη προς νέα δράση**

1.4. Στόχοι

1.4.1. Ο(οι) πολυετής(είς) στρατηγικός(οί) στόχος(οι) της Επιτροπής που αφορά η πρόταση/πρωτοβουλία

Σκοπός της προτεινόμενης οδηγίας είναι να εξασφαλιστεί **κοινό υψηλό επίπεδο** ασφάλειας δικτύων και πληροφοριών (**NIS**) **σε ολόκληρη την ΕΕ**.

1.4.2. Ειδικοί στόχοι και σχετικές δραστηριότητες ΔΒΔ/ΠΒΔ

Η πρόταση θεσπίζει μέτρα για τη διασφάλιση κοινού υψηλού επιπέδου ασφάλειας των δικτύων και των συστημάτων πληροφοριών σε ολόκληρη την Ένωση.

Οι ειδικοί στόχοι είναι οι εξής:

1. Να καθιερωθεί ελάχιστο επίπεδο ΑΔΠ στα κράτη μέλη και, συνεπώς, να αυξηθεί το συνολικό επίπεδο ετοιμότητας και απόκρισης.

2. Να βελτιωθεί η συνεργασία για την ασφάλεια δικτύων και πληροφοριών σε επίπεδο ΕΕ με σκοπό την αποτελεσματική πάταξη διασυνοριακών συμβάντων και απειλών. Θα τεθεί σε εφαρμογή μια υποδομή για ασφαλή ανταλλαγή πληροφοριών προκειμένου να καταστεί δυνατή η ανταλλαγή ευαίσθητων και εμπιστευτικών πληροφοριών μεταξύ των αρμόδιων αρχών.

3. Να διαμορφωθεί κλίμα διαχείρισης κινδύνου και να βελτιωθεί η ανταλλαγή πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα.

Οικεία(-ες) δραστηριότητα(-ες) ΔΒΔ/ΠΒΔ

Η οδηγία καλύπτει οντότητες (εταιρείες και οργανισμούς, συμπεριλαμβανομένων ορισμένων ΜΜΕ) σε ορισμένους τομείς (ενέργεια, μεταφορές, τα πιστωτικά ιδρύματα και τα χρηματιστήρια, υγειονομική περίθαλψη και τους καταλύτες των νευραλγικών διαδικτυακών υπηρεσιών) όσο και των δημόσιων διοικήσεων. Εξετάζει συνδέσμους με την επιβολή του νόμου και την προστασία των δεδομένων, καθώς και παραμέτρους ΑΔΠ στις εξωτερικές σχέσεις.

---

37 ΔΒΔ: διαχείριση βάσει δραστηριοτήτων – ΠΒΔ: προϋπολογισμός βάσει δραστηριοτήτων.

38 Όπως αναφέρεται στο άρθρο 49 παράγραφος 6 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

09 – δίκτυα, περιεχόμενο και τεχνολογία επικοινωνιών

02 - επιχειρήσεις

32 - ενέργεια

06 - κινητικότητα και μεταφορές

17 – υγεία και προστασία των καταναλωτών

18 - εσωτερικές υποθέσεις

19 – εξωτερικές σχέσεις

33 - δικαιοσύνη

12 εσωτερική αγορά

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

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

Η προστασία των ευρωπαίων καταναλωτών, των επιχειρήσεων και των κυβερνήσεων κατά συμβάντων ΑΔΠ, απειλών και κινδύνων θα βελτιωθεί σε σημαντικό βαθμό.

Για περισσότερες λεπτομέρειες μπορείτε να ανατρέξετε στο τμήμα 8.2 (αντίκτυπος της επιλογής 2 – κανονιστική προσέγγιση) του εγγράφου εργασίας των υπηρεσιών της Επιτροπής για την εκτίμηση του αντίκτυπου που συνοδεύει την παρούσα νομοθετική πρόταση.

1.4.4. Δείκτες αποτελεσμάτων και αντίκτυπου

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

Για τους δείκτες παρακολούθησης και αξιολόγησης μπορείτε να ανατρέξετε στο τμήμα 10 της εκτίμησης επιπτώσεων.

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών

Κάθε κράτος μέλος πρέπει να διαθέτει:

- εθνική στρατηγική για την ασφάλεια δικτύων και πληροφοριών (ΑΔΠ) ·

- σχέδιο συνεργασίας για την ασφάλεια δικτύων και πληροφοριών ·

- αρμόδια εθνική αρχή ΑΔΠ · και

- ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT)

Σε επίπεδο ΕΕ, θα ζητηθεί από τα κράτη μέλη να συνεργάζονται μέσω δικτύου.

Η δημόσια διοίκηση και οι κύριοι ιδιωτικοί παράγοντες θα υποχρεούνται να εφαρμόζουν διαχείριση κινδύνου για την ΑΔΠ και να υποβάλουν σχετική έκθεση στις αρμόδιες αρχές για συμβάντα ΑΔΠ με σημαντικό αντίκτυπο.

1.5.2. Προστιθέμενη αξία παρέμβασης της ΕΕ

Δεδομένου του διασυνοριακού χαρακτήρα της NIS, οι αποκλίσεις στη σχετική νομοθεσία και πολιτική συνιστούν εμπόδιο για τις επιχειρήσεις που ασκούν δραστηριότητες σε πολλές χώρες, καθώς και για την επίτευξη παγκόσμιων οικονομιών κλίμακας. Μη παρέμβαση σε επίπεδο ΕΕ θα οδηγήσει σε κατάσταση όπου κάθε κράτος μέλος θα ενεργεί μεμονωμένα, μη λαμβάνοντας υπόψη την αλληλεξάρτηση μεταξύ των συστημάτων δικτύων και πληροφοριών.

Οι δηλωμένοι στόχοι μπορούν συνεπώς 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 πρόταση απορρέει από τη διαπίστωση, ύστερα από σχετική ανάλυση, ότι απαιτούνται ρυθμιστικές υποχρεώσεις ώστε να δημιουργηθούν ίσοι όροι ανταγωνισμού και να καλυφθούν ορισμένα νομοθετικά κενά. Στο πεδίο αυτό, μια καθαρά εθελούσια προσέγγιση οδήγησε σε συνεργασία μεταξύ λίγων μόνον κρατών μελών με υψηλό επίπεδο ικανοτήτων.

1.5.4. Συμβατότητα και ενδεχόμενη συνέργεια με άλλα κατάλληλα μέσα

Η πρόταση είναι απόλυτα συνεπής με το Ψηφιακό θεματολόγιο για την Ευρώπη και, συνεπώς, με την στρατηγική «Ευρώπη 2020». Είναι, επίσης, συνεπής και συμπληρώνει το κανονιστικό πλαίσιο της ΕΕ για τις ηλ-επικοινωνίες, την οδηγία της ΕΕ σχετικά με τις ευρωπαϊκές υποδομές ζωτικής σημασίας και την οδηγία της ΕΕ για την προστασία των δεδομένων.

Η πρόταση συνοδεύει και αποτελεί ουσιαστικό μέρος της ανακοίνωσης της Επιτροπής και του ύπατου εκπροσώπου της Ένωσης για τις εξωτερικές υποθέσεις και την πολιτική ασφάλειας σχετικά με την ευρωπαϊκή στρατηγική ασφάλειας του κυβερνοχώρου.

1.6. Διάρκεια και δημοσιονομικός αντίκτυπος της δράσης

– ☐ Πρόταση/πρωτοβουλία περιορισμένης διάρκειας

– ☐ Ισχύουσα πρόταση/πρωτοβουλία από την [HH/MM]EEEE έως την [HH/MM]EEEE

– ☐ Δημοσιονομικός αντίκτυπος από το EEEE μέχρι το EEEE

– ☒ Πρόταση/πρωτοβουλία απεριόριστης διάρκειας

– Η περίοδος μεταφοράς θα αρχίσει ευθύς μετά την έγκριση (εκτιμάται το 2015) και θα διαρκέσει για περίοδο 18 μηνών. Η εφαρμογή της οδηγίας θα αρχίσει, ωστόσο, μετά την έγκρισή της και θα συνεπάγεται τη δημιουργία της ασφαλούς υποδομής που θα υποστηρίξει τη συνεργασία των κρατών μελών.

– και στη συνέχεια λειτουργία με κανονικό ρυθμό.

1.7. Προβλεπόμενοι τρόποι διαχείρισης[39]

– ☒ Κεντρική άμεση διαχείριση από την Επιτροπή

– ☒ Κεντρική έμμεση διαχείριση με ανάθεση καθηκόντων εκτέλεσης σε:

– ☐εκτελεστικούς οργανισμούς

– ☒ – οργανισμούς που έχουν συστήσει οι Κοινότητες[40]

– ☐ εθνικούς δημόσιους οργανισμούς / οργανισμούς με αποστολή δημόσιας υπηρεσίας

– ☐ πρόσωπα επιφορτισμένα με την εκτέλεση συγκεκριμένων δράσεων δυνάμει του τίτλου V της συνθήκης για την Ευρωπαϊκή Ένωση, όπως προσδιορίζονται στην αντίστοιχη βασική πράξη κατά την έννοια του άρθρου 49 του δημοσιονομικού κανονισμού.

– ☐ Επιμερισμένη διαχείριση με τα κράτη μέλη

– ☐ Αποκεντρωμένη διαχείριση με τρίτες χώρες

– ☐ Από κοινού διαχείριση με διεθνείς οργανισμούς, συμπεριλαμβανομένου του Ευρωπαϊκού Οργανισμού Διαστήματος

Αν αναφέρονται περισσότεροι τρόποι διαχείρισης, παρακαλείσθε να τους διευκρινίσετε στο τμήμα «Παρατηρήσεις».

Σχόλια:

Ο ENISA, αποκεντρωμένος οργανισμός που συστάθηκε από τις Κοινότητες, μπορεί να επικουρήσει τα κράτη μέλη και την Επιτροπή κατά την εφαρμογή της οδηγίας βάσει της εντολής του και με αναδιάταξη πόρων που προβλέπεται από το ΠΔΠ 2014-2020 για τον συγκεκριμένο οργανισμό.

[39] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης, καθώς και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον δικτυακό τόπο BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Όπως αναφέρονται στο άρθρο 185 του δημοσιονομικού κανονισμού.

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Διατάξεις στον τομέα της παρακολούθησης και της υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι των διατάξεων αυτών.

Η Επιτροπή διεξάγει περιοδική επανεξέταση της λειτουργίας της παρούσας οδηγίας και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.

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

Στην πρόταση για τη CEF προβλέπεται επίσης η δυνατότητα αξιολόγησης των μεθόδων εκτέλεσης των έργων, καθώς και των επιπτώσεων της υλοποίησής τους, ώστε να αποτιμάται κατά πόσον επιτεύχθηκαν οι στόχοι, περιλαμβανομένων εκείνων που αφορούν την προστασία του περιβάλλοντος.

2.2. Σύστημα διαχείρισης και ελέγχου

2.2.1. Κίνδυνος που έχει εντοπιστεί

- καθυστερήσεις στην υλοποίηση της οικοδόμησης ασφαλούς υποδομής

2.2.2. Προβλεπόμενες μέθοδοι ελέγχου

Οι συμφωνίες και αποφάσεις για την εφαρμογή των ενεργειών οι οποίες υπάγονται σε CEF θα προβλέπουν την εποπτεία και τον οικονομικό έλεγχο από μέρους της Επιτροπής ή από οποιονδήποτε εκπρόσωπο εξουσιοδοτημένο από την Επιτροπή, καθώς και λογιστικούς ελέγχους από το Ελεγκτικό Συνέδριο και επιτόπιους ελέγχους που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF).

2.2.3. Κόστος και οφέλη των ελέγχων και πιθανό ποσοστό μη συμμόρφωσης

Με εκ των προτέρων και εκ των υστέρων ελέγχους βάσει κινδύνου και με τη δυνατότητα επιτόπιων ελέγχων θα διασφαλιστεί ότι το κόστος των ελέγχων θα είναι εύλογο.

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας.

Η Επιτροπή λαμβάνει τα κατάλληλα μέτρα εξασφαλίζοντας ότι, κατά την υλοποίηση της δράσης που χρηματοδοτείται δυνάμει της παρούσας οδηγίας, προστατεύονται τα οικονομικά συμφέροντα της Ένωσης με την εφαρμογή προληπτικών μέτρων κατά της απάτης, της διαφθοράς και κάθε άλλης παράνομης δραστηριότητας, με τη διενέργεια αποτελεσματικών ελέγχων και, εφόσον διαπιστωθούν παρατυπίες, με την ανάκτηση των αχρεωστήτως καταβληθέντων ποσών, καθώς επίσης, κατά περίπτωση, με την επιβολή αποτελεσματικών, αναλογικών και αποτρεπτικών κυρώσεων.

Η Επιτροπή ή οι αντιπρόσωποί της και το Ελεγκτικό Συνέδριο έχουν την εξουσία να ελέγχουν, βάσει δικαιολογητικών καθώς και επιτόπιων ελέγχων, όλους τους δικαιούχους επιχορηγήσεων, τους εργολάβους και τους υπεργολάβους που έχουν λάβει πόρους της Ένωσης κατ' εφαρμογή [της παρούσας απόφασης / του παρόντος κανονισμού].

Η Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) δύναται να διενεργεί επιτόπιους ελέγχους και επιθεωρήσεις στους οικονομικούς παράγοντες που έχουν σχέση, άμεσα ή έμμεσα, με τη χρηματοδότηση αυτή, σύμφωνα με τις διαδικασίες

που καθορίζονται στον κανονισμό (Ευρατόμ, ΕΚ) αριθ. 2185/96, με στόχο τη διαπίστωση τυχόν απάτης, δωροδοκίας ή οποιασδήποτε άλλης παράνομης ενέργειας εις βάρος των οικονομικών συμφερόντων της Ένωσης σε σχέση με συμφωνία ή απόφαση επιχορήγησης ή με σύμβαση που αφορά χρηματοδότηση από μέρους της Ένωσης.

Με την επιφύλαξη των ανωτέρω παραγράφων, οι συμφωνίες συνεργασίας με τρίτες χώρες και διεθνείς οργανισμούς και οι συμφωνίες επιχορήγησης και οι αποφάσεις επιχορήγησης, καθώς και οι συμβάσεις που απορρέουν από την εφαρμογή του παρόντος κανονισμού εξουσιοδοτούν ρητά την Επιτροπή, το Ελεγκτικό Συνέδριο και την OLAF να διεξάγουν τους εν λόγω λογιστικούς ελέγχους, επιτόπιους ελέγχους και επιθεωρήσεις.

Η CEF προβλέπει ότι η σύναψη συμβάσεων για επιχορηγήσεις και δημόσιες συμβάσεις θα βασίζεται σε τυποποιημένα μοντέλα, τα οποία θα καθορίζουν τα γενικώς ισχύοντα μέτρα καταπολέμησης της απάτης.

3. ΕΚΤΙΜΩΜΕΝΟΣ ΔΗΜΟΣΙΟΝΟΜΙΚΟΣ ΑΝΤΙΚΤΥΠΟΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

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

- Υφιστάμενες γραμμές του προϋπολογισμού

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

Τομέας του πολυετούς δημοσ/κού πλαισίου	Γραμμή προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθ. [Περιγραφή… ... …]	ΔΠ/ΜΔΠ (41)	από χώρες ΕΖΕΣ[42]	Από υποψήφιες χώρες[43]	από τρίτες χώρες	κατά την έννοια του άρθρου 18 παράγραφος 1 στοιχείο αα) του δημοσιονομικού κανονισμού
	09 03 02 Προώθηση της διασύνδεσης και της διαλειτουργικότητας των επιγραμμικών εθνικών δημόσιων υπηρεσιών, καθώς και της πρόσβασης σε αυτά τα δίκτυα.	Αριθμός	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

- Νέες γραμμές του προϋπολογισμού, των οποίων έχει ζητηθεί η δημιουργία (δεν εφαρμόζεται)

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

Τομέας του πολυετούς δημοσ/κού πλαισίου	Γραμμή προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθ. [Ονομασία…...….]	ΔΠ/ΜΔΠ	χωρών της ΕΖΕΣ	υποψήφιων χωρών	από τρίτες χώρες	κατά την έννοια του άρθρου 18 παράγραφος 1 στοιχείο αα) του δημοσιονομικού κανονισμού
	[XX.YY.YY.YY]		ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ

41 ΔΠ= Διαχωριζόμενες πιστώσεις / ΜΔΠ= Μη διαχωριζόμενες πιστώσεις

42 ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.

43 Υποψήφιες χώρες και, εφόσον ενδείκνυται, δυνάμει υποψήφιες χώρες των Δυτικών Βαλκανίων.

3.2. Εκτιμώμενος αντίκτυπος στις δαπάνες

3.2.1. Συνοπτική παρουσίαση του εκτιμώμενου αντίκτυπου στις δαπάνες

Σε εκατ. ευρώ (με 3 δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου:	1	Έξυπνη και χωρίς αποκλεισμούς μεγέθυνση

ΓΔ: <…….>			2015* [44]	Έτος **2016**	Έτος **2017**	Έτος **2018**	Επόμενα έτη (2019-2021) και μετέπειτα			**ΣΥΝΟΛΟ**
• Επιχειρησιακές πιστώσεις										
09 03 02	Αναλήψεις υποχρεώσεων	(1)	1.250**	0.000						**1.250**
	Πληρωμές	(2)	0.750	0.250	0.250					**1.250**
Πιστώσεις διοικητικού χαρακτήρα χρηματοδοτούμενες από το κονδύλιο ειδικών προγραμμάτων[45]			**0.000**							**0.000**
Αριθμός γραμμής του προϋπολογισμού		(3)	**0.000**							**0.000**
ΣΥΝΟΛΟ πιστώσεων για τη ΓΔ <….>	Αναλήψεις υποχρεώσεων	= 1 + 1α + 3	1.250	0.000						**1.250**
	Πληρωμές	= 2 + 2α +3	0.750	0.250	0.250					**1.250**

• ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων	Αναλήψεις	(4)	1.250	0.000						**1.250**

[44] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας.

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

	υποχρεώσεων										
	Πληρωμές	(5)	0.750	0.250	0.250						**1.250**
• ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων		(6)	**0.000**								
ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 1 του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων	=4+ 6	1.250	0.000							**1.250**
	Πληρωμές	=5+ 6	0.750	0.250	0.250						**1.250**

* Η ακριβής χρονική στιγμή θα εξαρτηθεί από την ημερομηνία έγκρισης της πρότασης από την νομοθετική αρχή (δηλαδή, εάν η οδηγία θα εγκριθεί κατά τη διάρκεια του 2014, η προσαρμογή της υφιστάμενης υποδομής θα αρχίσει το 2015, αλλιώς, ένα έτος αργότερα).

* * εάν τα κράτη μέλη επιλέξουν να χρησιμοποιήσουν υπάρχουσα υποδομή και να καλύψουν το εφάπαξ κόστος προσαρμογής στο πλαίσιο του προϋπολογισμού της ΕΕ, όπως εξηγείται στο 1.4.3 και 1.7, το κόστος προσαρμογής ενός δικτύου για την υποστήριξη της συνεργασίας μεταξύ των κρατών μελών, σύμφωνα με το κεφάλαιο ΙΙΙ της οδηγίας (έγκαιρη προειδοποίηση, συντονισμένη απόκριση κλπ.) εκτιμάται σε 1.250.000 ευρώ. Το ποσό αυτό είναι ελαφρώς υψηλότερο από το αναφερόμενο στην εκτίμηση του αντίκτυπου («περίπου 1 εκατομμύριο ευρώ»), δεδομένου ότι βασίζεται σε ακριβέστερη εκτίμηση των απαραίτητων δομοστοιχείων για την εν λόγω υποδομή. Τα αναγκαία δομοστοιχεία και οι σχετικές δαπάνες βασίζονται σε εκτίμηση του ΚΚΕρ, με βάση την εμπειρία του στην ανάπτυξη παρόμοιων συστημάτων για άλλα πεδία, όπως η δημόσια υγεία, και θα περιλαμβάνει τα ακόλουθα: σύστημα ταχείας ειδοποίησης και κοινοποίησης για ΑΔΠ (275 000 ευρώ) · μηχανισμό ανταλλαγής πληροφοριών (400.000 ευρώ) · σύστημα έγκαιρου συναγερμού και απόκρισης (275.000 ευρώ) · θάλαμο επιχειρήσεων (300.000 ευρώ) για συνολικό ποσό 1.250.000 ευρώ. Αναλυτικότερο σχέδιο υλοποίησης αναμένεται στην επικείμενη μελέτη σκοπιμότητας στο πλαίσιο της ειδικής σύμβασης SMART 2012/0010: «Μελέτη σκοπιμότητας και προπαρασκευαστικές δραστηριότητες για την υλοποίηση ενός ευρωπαϊκού συστήματος έγκαιρης προειδοποίησης και απόκρισης εναντίον επιθέσεων στον κυβερνοχώρο και διαταραχών».

Αν η πρόταση/πρωτοβουλία επηρεάζει περισσότερους από έναν τομείς:

• ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων	Αναλήψεις υποχρεώσεων	(4)	0.000	0.000						
	Πληρωμές	(5)	0.000	0.000						
• ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων		(6)	**0.000**	**0.000**						
ΣΥΝΟΛΟ πιστώσεων	Αναλήψεις υποχρεώσεων	=4+ 6	1.250	0.000						1.250

των ΤΟΜΕΩΝ 1 έως 4 του πολυετούς δημοσιονομικού πλαισίου (Ποσό αναφοράς)	Πληρωμές	=5+ 6	0.750	0.250	0.250					1.250

Τομέας του πολυετούς δημοσιονομικού πλαισίου	**5**	«Δαπάνες διοικητικής λειτουργίας»

Σε εκατ. ευρώ (με 3 δεκαδικά ψηφία)

		Έτος **2015**	Έτος **2016**	Έτος **2017**	Έτος **2018**	Επόμενα έτη (2019-2021) και μετέπειτα			**ΣΥΝΟΛΟ**
ΓΔ: CNECT									
• Ανθρώπινοι πόροι		0.572	0.572	0.572	0.572	0.572	0.572	**0.572**	**4.004**
• Άλλες διοικητικές δαπάνες		0.318	0.118	0.318	0.118	0.318	0.118	**0.118**	**1.426**
ΣΥΝΟΛΟ ΓΔ CNECT	Πιστώσεις	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

ΣΥΝΟΛΟ πιστώσεων για τον ΤΟΜΕΑ 5 του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο πιστώσεων ανάληψης υποχρεώσεων = Σύνολο πληρωμών)	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Σε εκατ. ευρώ (με 3 δεκαδικά ψηφία)

		Έτος **2015**[46]	Έτος **2016**	Έτος **2017**	Έτος **2018**	Επόμενα έτη (2019-2021) και μετέπειτα			**ΣΥΝΟΛΟ**
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 5 του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων	2.140	0.690	0.890	0.690	0.890	0.690	0.690	**6.680**
	Πληρωμές	1.640	0.940	1.140	0.690	0.890	0.690	0.690	**6.680**

[46] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας.

3.2.2. Εκτιμώμενος αντίκτυπος στις επιχειρησιακές πιστώσεις

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

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

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

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα ⇩			Έτος **2015***		Έτος **2016**		Έτος **2017**		Έτος **2018**		Επόμενα έτη (2019-2021) και μετέπειτα						**ΣΥΝΟΛΟ**	
	ΑΠΟΤΕΛΕΣΜΑΤΑ (OUTPUTS)																	
	Είδος [47]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθμός	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ ΑΡΙΘ. 2[48] Ασφαλής υποδομής ανταλλαγής πληροφοριών																		
- Αποτελέσματα	Προσαρμογή των υποδο																	
Υποσύνολο για ειδικό στόχο αριθ. 2			1	1.250**													1	1.250
ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ				1.250														1.250

[47] Τα αποτελέσματα αφορούν τα προϊόντα και τις υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών σπουδαστών που χρηματοδοτήθηκαν, αριθμός χλμ οδών που κατασκευάστηκαν κ.λπ).

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

* Η ακριβής χρονική στιγμή θα εξαρτηθεί από την ημερομηνία έγκρισης της πρότασης από την νομοθετική αρχή (δηλ., εάν η οδηγία εγκριθεί κατά τη διάρκεια του 2014, η προσαρμογή της υφιστάμενης υποδομής θα αρχίσει το 2015, αλλιώς, ένα έτος αργότερα).

** Βλ. σημείο 3.2.1

3.2.3. Εκτιμώμενος αντίκτυπος στις πιστώσεις διοικητικού χαρακτήρα

3.2.3.1. Συνοπτική παρουσίαση

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

– ☑ Η πρόταση/πρωτοβουλία απαιτεί τη χρήση διοικητικών πιστώσεων, όπως εξηγείται παρακάτω:

Σε εκατ. ευρώ (με 3 δεκαδικά ψηφία)

	Έτος **2015**[49]	Έτος **2016**	Έτος **2017**	Έτος **2018**	Επόμενα έτη (2019-2021) και μετέπειτα			**ΣΥΝΟΛΟ**
ΤΟΜΕΑΣ 5 του πολυετούς δημοσιονομικού πλαισίου								
Ανθρώπινοι πόροι	0.572	0.572	0.572	0.572	0.572	0.572	0.572	**4.004**
Άλλες διοικητικές δαπάνες	0.318	0.118	0.318	0.118	0.318	0.118	0.118	**1.426**
Υποσύνολο ΤΟΜΕΑ 5 του πολυετούς δημοσιονομικού πλαισίου	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Εκτός του ΤΟΜΕΑ 5[50] **του πολυετούς δημοσιονομικού πλαισίου**								
Ανθρώπινοι πόροι	0.000	0.000						**0.000**
Λοιπές δαπάνες διοικητικού χαρακτήρα								
Υποσύνολο εκτός ΤΟΜΕΑ 5 του πολυετούς δημοσιονομικού πλαισίου	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

ΣΥΝΟΛΟ	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Οι ανάγκες σε διοικητικές πιστώσεις θα καλυφθούν από τις πιστώσεις της ΓΔ CNECT που έχουν ήδη διατεθεί για τη διαχείριση της δράσης ή/και που έχουν ανακατανεμηθεί εντός της ΓΔ, μαζί, εφόσον απαιτηθεί, με κάθε πρόσθετο κονδύλιο που θα μπορούσε να χορηγηθεί στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της διαδικασίας ετήσιας χορήγησης και βάσει των υφιστάμενων ορίων του προϋπολογισμού.

[49] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας.

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

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) θα μπορούσε να συνδράμει τα κράτη μέλη και την Επιτροπή κατά την εφαρμογή της οδηγίας βάσει της εντολής του και με ανακατανομή των πόρων στο πλαίσιο του πολυετούς δημοσιονομικού πλαισίου 2014-2020 για τον εν λόγω οργανισμό, δηλαδή, χωρίς πρόσθετα κονδύλια, δημοσιονομικά ή ανθρώπινων πόρων.

3.2.3.2. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους

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

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρωπίνων πόρων της Επιτροπής, όπως εξηγείται παρακάτω:

Καταρχήν δεν θα απαιτηθεί πρόσθετο εργατικό δυναμικό. Οι απαιτούμενες ανάγκες σε ανθρώπινους πόρους θα είναι ιδιαίτερα περιορισμένες και θα καλυφθούν από προσωπικό της ΓΔ στο οποίο έχει ήδη ανατεθεί η διαχείριση της δράσης.

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

	Έτος **2015**	Έτος **2016**	Έτος **2017**	Έτος **2018**	Επόμενα έτη (2019-2021) και μετέπειτα		
• Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)							
09 01 01 01 (στην έδρα ή στα γραφεία αντιπροσωπείας της Επιτροπής)	4	4	4	4	4	4	4
XX 01 05 01 (Σε αντιπροσωπείες)							
XX 01 05 01 (Έμμεση έρευνα)							
10 01 05 01 (Άμεση έρευνα)							
• Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)[51]							
09 01 02 01 (ΣΥ, ΠΠ, ΑΕΕ από το «συνολικό κονδύλιο»)	1	1	1	1	1	1	1
XX 01 02 02 (ΣΥ, ΠΠ, ΝΕΑ, ΤΥ και ΑΕΕ στις αντιπροσωπείες)							
XX 01 04 ***α*** [52] - στην έδρα[53]							
XX 01 04 ***α*** [52] - σε αντιπροσωπείες							
XX 01 05 02 (ΣΥ, ΠΠ, ΑΕΕ - Έμμεση έρευνα)							
10 01 05 02 (ΣΥ, ΠΠ, ΑΕΕ - Άμεση έρευνα)							
Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν)							
ΣΥΝΟΛΟ	**5**	**5**	**5**	**5**	**5**	**5**	**5**

51 CA = Συμβασιούχος υπάλληλος· INT= προσωρινό προσωπικό («*Intérimaire*»)· JED = "*Jeune Expert en Délégation*" (Νεαρός εμπειρογνώμονας σε αντιπροσωπεία). LA = Τοπικός υπάλληλος, SNE= Seconded National Expert (αποσπασμένος εθνικός εμπειρογνώμονας)

52 Επιμέρους ανώτατο όριο εξωτερικού προσωπικού βάσει επιχειρησιακών πιστώσεων (πρώην γραμμές «ΒΑ»).

53 Κυρίως για τα Διαρθρωτικά Ταμεία, το Ευρωπαϊκό Γεωργικό Ταμείο Αγροτικής Ανάπτυξης (ΕΓΤΑΑ) και το Ευρωπαϊκό Ταμείο Αλιείας (ΕΤΑ).

XX είναι το πεδίο πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από προσωπικό της ΓΔ που απασχολείται ήδη στη διαχείριση της δράσης ή/και που έχει μετακινηθεί στο πλαίσιο της ίδιας ΓΔ και θα συμπληρωθούν, ενδεχομένως, από όλα τα συμπληρωματικά κονδύλια που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση της δράσης ΓΔ, στο πλαίσιο της ετήσιας διαδικασίας κατανομής των πιστώσεων με βάση τους δημοσιονομικούς περιορισμούς.

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) θα μπορούσε να συνδράμει τα κράτη μέλη και την Επιτροπή κατά την εφαρμογή της οδηγίας βάσει της εντολής του και με ανακατανομή των πόρων στο πλαίσιο του πολυετούς δημοσιονομικού πλαισίου 2014-2020 για τον εν λόγω οργανισμό, δηλαδή, χωρίς πρόσθετα κονδύλια, δημοσιονομικά ή ανθρώπινων πόρων.

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	Προετοιμασία των πράξεων κατ'εξουσιοδότηση σύμφωνα με το άρθρο 14 παράγραφος 3) - Προετοιμασία εκτελεστικών πράξεων σύμφωνα με τα άρθρα 8, 9 παράγραφος 2, 12, 14 παράγραφος 5, 16 - Συμβολή στη συνεργασία μέσω του δικτύου, τόσο σε πολιτικό όσο και σε επιχειρησιακό επίπεδο. - Συμμετοχή σε διεθνείς διαπραγματεύσεις και σε ενδεχόμενη σύναψη διεθνών συμφωνιών
Εξωτερικό προσωπικό	Υποστήριξη όλων των ανωτέρω καθηκόντων κατά περίπτωση.

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.

Η εκτιμώμενη δημοσιονομική επίπτωση στις επιχειρησιακές δαπάνες της πρότασης θα προκύψει εάν τα κράτη μέλη επιλέξουν να προσαρμόσουν την υπάρχουσα υποδομή και αναθέσουν στην Επιτροπή να υλοποιήσει την προσαρμογή της υπό το ΠΔΠ 2014-2020. Το εφάπαξ κόστος θα καλυφθεί στο πλαίσιο της CEF υπό τον όρο ότι διατίθενται επαρκή κονδύλια. Εναλλακτικά, τα κράτη μέλη μπορούν να μοιραστούν, είτε το κόστος προσαρμογής των υποδομών είτε τις δαπάνες για τη δημιουργία νέας υποδομής.

– ☐ Η πρόταση/πρωτοβουλία απαιτεί εφαρμογή του μέσου ευελιξίας ή αναθεώρηση του πολυετούς δημοσιονομικού πλαισίου[54].

Δεν συμπληρώνεται.

3.2.5. Συμμετοχή τρίτων μερών στη χρηματοδότηση

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

3.3. Εκτιμώμενος δημοσιονομικός αντίκτυπος στα έσοδα

– ☑ Η πρόταση/πρωτοβουλία δεν έχει κανένα δημοσιονομικό αντίκτυπο στα έσοδα.

[54] Βλ. σημεία 19 και 24 της διοργανικής συμφωνίας.