ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ΠΑΡΑΡΤΗΜΑ

της

ΑΝΑΚΟΙΝΩΣΗΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ

Αξιοποιώντας την ΑΔΠ στο έπακρον – Για την αποτελεσματική εφαρμογή της οδηγίας (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΑΡΑΡΤΗΜΑ

1. Εισαγωγή

Σκοπός του παρόντος παραρτήματος είναι να συμβάλει στην αποτελεσματική υλοποίηση, εφαρμογή και επιβολή της οδηγίας ΑΔΠ (ΕΕ) 2016/1148 σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση[1] (εφεξής «οδηγία ΑΔΠ» ή «οδηγία») και να βοηθήσει τα κράτη μέλη να διασφαλίσουν την αποτελεσματική εφαρμογή του δικαίου της ΕΕ. Πιο συγκεκριμένα, το παράρτημα έχει τρεις ειδικούς στόχους: α) να βοηθήσει τις εθνικές αρχές να κατανοήσουν καλύτερα τις υποχρεώσεις που υπέχουν δυνάμει της οδηγίας, β) να διασφαλίσει την αποτελεσματική επιβολή των υποχρεώσεων που προβλέπει η οδηγία για τις οντότητες που υπέχουν υποχρεώσεις δυνάμει των απαιτήσεων ασφάλειας και κοινοποίησης συμβάντων και γ) να συμβάλει γενικότερα στη δημιουργία κλίματος ασφάλειας δικαίου για όλους τους εμπλεκόμενους φορείς.

Για τον σκοπό αυτόν, το παρόν παράρτημα παρέχει καθοδήγηση για τις πτυχές που παρατίθενται ακολούθως, οι οποίες είναι καθοριστικής σημασίας για την επίτευξη του στόχου που επιδιώκει η οδηγία ΑΔΠ, ήτοι την επίτευξη υψηλού κοινού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών εντός της Ένωσης, με σκοπό την καλύτερη λειτουργία της κοινωνίας και της οικονομίας της ΕΕ:

- την υποχρέωση των κρατών μελών να υιοθετήσουν εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών (ενότητα 2)·
- τον ορισμό εθνικών αρμόδιων αρχών, ενιαίων κέντρων επαφής και ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (ενότητα 3)·
- τις απαιτήσεις ασφάλειας και κοινοποίησης συμβάντων για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και για τους παρόχους ψηφιακών υπηρεσιών (ενότητα 4)· και
- τη σχέση μεταξύ της οδηγίας ΑΔΠ και λοιπής νομοθεσίας (ενότητα 5)

Για τη σύνταξη του παρόντος εγγράφου καθοδήγησης, η Επιτροπή χρησιμοποίησε τις συνεισφορές και αναλύσεις που συλλέχθηκαν κατά την προετοιμασία της οδηγίας, καθώς και τις συνεισφορές του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών («ENISA») και της ομάδας συνεργασίας. Αξιοποίησε επίσης τις εμπειρίες συγκεκριμένων κρατών μελών. Η Επιτροπή έλαβε επιπλέον υπόψη, όπου απαιτήθηκε, τις κατευθυντήριες αρχές για την ερμηνεία του δικαίου της ΕΕ: τη διατύπωση, το πλαίσιο και τους στόχους της οδηγίας ΑΔΠ. Καθώς η οδηγία δεν έχει μεταφερθεί ακόμη στα εθνικά δίκαια, δεν έχει εκδοθεί μέχρι στιγμής καμία απόφαση του Δικαστηρίου της Ευρωπαϊκής

[1] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. Η οδηγία άρχισε να ισχύει στις 8 Αυγούστου 2016.

Ένωσης (ΔΕΕ) ή εθνικών δικαστηρίων σχετικά με αυτήν. Δεν έχει επομένως διαμορφωθεί ακόμη σχετική νομολογία που να μπορεί να χρησιμοποιηθεί για σκοπούς καθοδήγησης.

Η συγκέντρωση των σχετικών πληροφοριών σε ενιαίο έγγραφο αναμένεται να βοηθήσει τα κράτη μέλη να αποκτήσουν ολοκληρωμένη εικόνα της οδηγίας. Θα τα διευκολύνει επιπλέον να λάβουν υπόψη τις εν λόγω πληροφορίες κατά την εκπόνηση της συναφούς εθνικής νομοθεσίας τους. Ταυτόχρονα, η Επιτροπή υπογραμμίζει ότι το παρόν παράρτημα δεν είναι δεσμευτικό και δεν επιδιώκει να δημιουργήσει νέους κανόνες. Η τελική αρμοδιότητα της ερμηνείας του δικαίου της ΕΕ ανήκει στο ΔΕΕ.

2. Εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών

Σύμφωνα με το άρθρο 7 της οδηγίας ΑΔΠ, τα κράτη μέλη οφείλουν να θεσπίσουν εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών, όρος που μπορεί να θεωρηθεί ισοδύναμος του όρου «εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο» («ΕΣΑΚ»). Η εθνική στρατηγική εξυπηρετεί ουσιαστικά τον σκοπό του καθορισμού των στρατηγικών στόχων και των κατάλληλων μέτρων πολιτικής και κανονιστικής ρύθμισης για την ασφάλεια στον κυβερνοχώρο. Η έννοια της ΕΣΑΚ χρησιμοποιείται ευρέως τόσο διεθνώς όσο και στην Ευρώπη, ιδίως δε στο πλαίσιο των εργασιών του ENISA σε συνεργασία με τα κράτη μέλη για τη χάραξη των συναφών εθνικών στρατηγικών τους. Προϊόν των εν λόγω εργασιών ήταν δε πρόσφατα η σύνταξη επικαιροποιημένου οδηγού ορθών πρακτικών ανάπτυξης ΕΣΑΚ[2].

Στην παρούσα ενότητα, η Επιτροπή εξειδικεύει τους τρόπους με τους οποίους η οδηγία ΑΔΠ συμβάλλει στην ενίσχυση της ετοιμότητας των κρατών μελών μέσω της επιβολής στα τελευταία της υποχρέωσης να θεσπίσουν στιβαρές εθνικές στρατηγικές για την ασφάλεια συστημάτων δικτύου και πληροφοριών (άρθρο 7). Στην παρούσα ενότητα εξετάζονται οι ακόλουθες πτυχές: α) το πεδίο εφαρμογής της στρατηγικής και β) το περιεχόμενο και η διαδικασία έγκρισης.

Όπως περιγράφεται εκτενέστερα ακολούθως, η ορθή μεταφορά στο εθνικό δίκαιο του άρθρου 7 της οδηγίας ΑΔΠ είναι καθοριστικής σημασίας για την επίτευξη των στόχων της οδηγίας και καθιστά αναγκαία τη διάθεση επαρκών οικονομικών και ανθρώπινων πόρων για τον συγκεκριμένο σκοπό.

2.1. Το πεδίο εφαρμογής της εθνικής στρατηγικής

Σύμφωνα με τη διατύπωση του άρθρου 7, με την υποχρέωση θέσπισης ΕΣΑΚ καλύπτονται μόνο οι τομείς που αναφέρονται στο παράρτημα ΙΙ (ήτοι ενέργεια, μεταφορές, τράπεζες, χρηματοπιστωτικές αγορές, υγεία, προμήθεια και διανομή πόσιμου νερού και ψηφιακή υποδομή) και οι υπηρεσίες που αναφέρονται στο παράρτημα ΙΙΙ (επιγραμμική αγορά, επιγραμμική μηχανή αναζήτησης και υπηρεσία νεφοϋπολογιστικής).

[2] ENISA, *National Cyber-Security Strategy Good Practice* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Το άρθρο 3 της οδηγίας προβλέπει ρητά την αρχή της ελάχιστης εναρμόνισης, σύμφωνα με την οποία τα κράτη μέλη μπορούν να θεσπίζουν ή να διατηρούν διατάξεις με στόχο την επίτευξη υψηλότερου επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών. Η εφαρμογή της εν λόγω αρχής στην υποχρέωση θέσπισης «ΕΣΑΚ» παρέχει στα κράτη μέλη τη δυνατότητα να συμπεριλάβουν περισσότερους τομείς και υπηρεσίες από αυτούς που περιλαμβάνονται αντίστοιχα στα παραρτήματα ΙΙ και ΙΙΙ της οδηγίας.

Κατά την άποψη της Επιτροπής και υπό το πρίσμα του στόχου της οδηγίας ΑΔΠ, ήτοι της επίτευξης υψηλού κοινού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών εντός της Ένωσης[3], θα ήταν σκόπιμο να αναπτυχθεί μια εθνική στρατηγική η οποία θα καλύπτει όλες τις σχετικές διαστάσεις της κοινωνίας και της οικονομίας, και όχι μόνο τους τομείς και τις ψηφιακές υπηρεσίες που αναφέρονται αντίστοιχα στα παραρτήματα ΙΙ και ΙΙΙ της οδηγίας ΑΔΠ. Τούτο συνάδει δε με τις βέλτιστες πρακτικές που εφαρμόζονται διεθνώς (βλ. κατευθυντήριες γραμμές της Διεθνούς Ένωσης Τηλεπικοινωνιών (ΔΕΤ) και σχετική ανάλυση του ΟΟΣΑ) και με την οδηγία ΑΔΠ.

Όπως επεξηγείται εκτενέστερα ακολούθως, αυτό ισχύει ιδίως για τους φορείς δημόσιας διοίκησης που είναι αρμόδιοι για τομείς και υπηρεσίες πέραν εκείνων που αναφέρονται στα παραρτήματα ΙΙ και ΙΙΙ της οδηγίας. Οι φορείς δημόσιας διοίκησης επεξεργάζονται συνήθως ευαίσθητες πληροφορίες, γεγονός που δικαιολογεί την ανάγκη να καλύπτονται από ΕΣΑΚ και από σχέδια διαχείρισης που αποτρέπουν τις διαρροές και διασφαλίζουν την κατάλληλη προστασία των εν λόγω πληροφοριών.

2.2. Περιεχόμενο και διαδικασία έγκρισης των εθνικών στρατηγικών

Σύμφωνα με το άρθρο 7 της οδηγίας ΑΔΠ, μια ΕΣΑΚ πρέπει να περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:

i) τους στόχους και τις προτεραιότητες της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών·
ii) το πλαίσιο διακυβέρνησης για την επίτευξη του στόχου και των προτεραιοτήτων της εθνικής στρατηγικής·
iii) τον προσδιορισμό των μέτρων ετοιμότητας, παρέμβασης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στο δημόσιο και ιδιωτικό τομέα·
iv) αναφορά των σχετικών προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και κατάρτισης·
v) αναφορά των σχεδίων έρευνας και ανάπτυξης·
vi) σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων· και
vii) κατάλογο των φορέων που εμπλέκονται στην υλοποίηση της στρατηγικής.

Εντούτοις, ούτε το άρθρο 7 ούτε η αντίστοιχη αιτιολογική σκέψη 29 εξειδικεύουν τις απαιτήσεις θέσπισης ΕΣΑΚ και, επιπλέον, δεν παρέχουν περισσότερες λεπτομέρειες σχετικά με το περιεχόμενό της. Όσον αφορά τη διαδικασία και πρόσθετα στοιχεία σχετικά με το περιεχόμενο της ΕΣΑΚ, η Επιτροπή εκτιμά ότι η προσέγγιση που παρατίθεται ακολούθως

[3] Βλ. άρθρο 1 παράγραφος 1.

αποτελεί κατάλληλη μέθοδο θέσπισης ΕΣΑΚ. Η εν λόγω εκτίμηση της Επιτροπής βασίζεται σε αναλύσεις κρατών μελών και σε εμπειρίες τρίτων χωρών όσον αφορά τους τρόπους ανάπτυξης των δικών τους στρατηγικών από κράτη μέλη. Πρόσθετη πηγή πληροφόρησης αποτελεί το εργαλείο κατάρτισης του ENISA σε θέματα ΕΣΑΚ, το οποίο είναι διαθέσιμο στον δικτυακό τόπο του οργανισμού και περιλαμβάνει βιντεοκλίπ και μεταφορτώσιμα μέσα[4].

2.3. Διαδικασία και θέματα προς εξέταση

Η κατάρτιση εθνικής στρατηγικής και η επακόλουθη έγκρισή της συνιστούν πολύπλοκη και πολύπλευρη διαδικασία, η οποία απαιτεί διαρκή δέσμευση και συνεργασία με τους εμπειρογνώμονες σε θέματα ασφάλειας στον κυβερνοχώρο, την κοινωνία πολιτών και την εθνική πολιτική διαδικασία προκειμένου να εξασφαλιστεί η αποτελεσματικότητα και η επιτυχία της. Απαραίτητη προϋπόθεση είναι η στήριξη του όλου εγχειρήματος από τις ανώτερες διοικητικές βαθμίδες του καθ' ύλην αρμόδιου υπουργείου, τουλάχιστον σε επίπεδο υπουργού ή σε ισοδύναμο επίπεδο, καθώς και η ανάληψη της συναφούς πολιτικής ευθύνης. Για την επιτυχημένη θέσπιση ΕΣΑΚ, θα μπορούσε να ληφθεί υπόψη η ακόλουθη διαδικασία πέντε βημάτων (βλ. σχήμα 1):

Πρώτο βήμα - **Θέσπιση κατευθυντήριων αρχών και στρατηγικών στόχων που προκύπτουν από τη στρατηγική**

Καταρχάς, οι αρμόδιες εθνικές αρχές θα πρέπει να προσδιορίσουν κάποια βασικά στοιχεία προς συμπερίληψη στην ΕΣΑΚ, συγκεκριμένα δε τα επιθυμητά αποτελέσματα, σύμφωνα με τη διατύπωση της οδηγίας (άρθρο 7 παράγραφος 1 στοιχείο α)) *«τους στόχους και τις προτεραιότητες»*, τους τρόπους με τους οποίους τα εν λόγω αποτελέσματα συμπληρώνουν τις εθνικές κοινωνικές και οικονομικές πολιτικές και κατά πόσο είναι συμβατά με τα προνόμια και τις υποχρεώσεις που απορρέουν από την ιδιότητα του κράτους μέλους της Ευρωπαϊκής Ένωσης. Οι στόχοι θα πρέπει να είναι συγκεκριμένοι, μετρήσιμοι, εφικτοί, ρεαλιστικοί και χρονικά προσδιορισμένοι (SMART). Χαρακτηριστικό παράδειγμα είναι το εξής: «*Θα μεριμνήσουμε ώστε αυτή η [χρονικά προσδιορισμένη] στρατηγική να στηριχθεί σε μια αυστηρή και ολοκληρωμένη σειρά μεθόδων μέτρησης της προόδου προς την κατεύθυνση των αποτελεσμάτων που καλούμαστε να επιτύχουμε*»[5]

Πέραν των προαναφερθέντων, θα πρέπει επίσης να αξιολογηθεί σε πολιτικό επίπεδο εάν είναι δυνατό να εξασφαλιστεί ικανός προϋπολογισμός ώστε να καταστεί δυνατή η διάθεση των απαιτούμενων πόρων για την εφαρμογή της στρατηγικής. Θα πρέπει ακόμη να γίνει περιγραφή του σκοπούμενου πεδίου εφαρμογής της στρατηγικής και των διαφόρων κατηγοριών ενδιαφερομένων από τον δημόσιο και ιδιωτικό τομέα που θα πρέπει να συμμετάσχουν στη σύνταξη των διαφόρων στόχων και μέτρων.

Το πρώτο αυτό στάδιο θα μπορούσε να υλοποιηθεί μέσω της διεξαγωγής εστιασμένων εργαστηρίων στα οποία θα συμμετέχουν ανώτερα στελέχη υπουργείων και πολιτικοί υπό τον

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

[5] Απόσπασμα από την εθνική στρατηγική του Ηνωμένου Βασιλείου για την ασφάλεια στον κυβερνοχώρο, 2016-2021, σελ. 67.

συντονισμό εξειδικευμένων επαγγελματιών σε θέματα κυβερνοχώρου οι οποίοι θα διαθέτουν αναπτυγμένες επικοινωνιακές δεξιότητες και θα είναι σε θέση να αναδείξουν τις επιπτώσεις που έχει για τις σύγχρονες ψηφιακές οικονομίες και κοινωνίες η παντελής έλλειψη ασφάλειας ή η ανεπαρκής ασφάλεια στον κυβερνοχώρο.

Δεύτερο βήμα - **Ανάπτυξη του περιεχομένου της στρατηγικής**

Η στρατηγική θα πρέπει να περιλαμβάνει υποστηρικτικά μέτρα, χρονικά προσδιορισμένες δράσεις και κύριους δείκτες επιδόσεων ώστε να μπορέσουν να γίνουν οι απαιτούμενες αξιολογήσεις, προσαρμογές και βελτιώσεις μετά την πάροδο καθορισμένης περιόδου εφαρμογής. Τα μέτρα αυτά θα πρέπει να στηρίζουν τον στόχο, τις προτεραιότητες και τα αποτελέσματα που ορίζονται ως κατευθυντήριες αρχές. Η ανάγκη συμπερίληψης υποστηρικτικών μέτρων προβλέπεται στο άρθρο 7 παράγραφος 1 στοιχείο γ) της οδηγίας ΑΔΠ.

Συνιστάται δε η σύσταση ομάδας συντονισμού υπό την προεδρία του καθ' ύλην αρμόδιου υπουργείου για τη διαχείριση της διαδικασίας σύνταξης και τη διευκόλυνση της υποβολής των σχετικών συνεισφορών. Ειδικότερα, θα μπορούσαν να συσταθούν διάφορες ομάδες σύνταξης αποτελούμενες από αρμόδιους κρατικούς υπαλλήλους και εμπειρογνώμονες για βασικά γενικά θέματα όπως, π.χ., εκτίμηση κινδύνου, σχέδια αντιμετώπισης απρόοπτων καταστάσεων, διαχείριση συμβάντων, ανάπτυξη δεξιοτήτων, ευαισθητοποίηση, έρευνα και βιομηχανική ανάπτυξη, κ.λπ. Κάθε τομέας χωριστά (π.χ. ενέργεια, μεταφορές κ.λπ.) θα μπορούσε επιπλέον να κληθεί να αξιολογήσει τις επιπτώσεις της δικής του συμμετοχής, μεταξύ άλλων ως προς τους πόρους, και να μεριμνήσει για τη συμμετοχή των ορισθέντων φορέων εκμετάλλευσης βασικών υπηρεσιών και των κύριων παρόχων ψηφιακών υπηρεσιών στον καθορισμό των προτεραιοτήτων και στην υποβολή προτάσεων κατά τη διαδικασία σύνταξης. Με δεδομένη την ανάγκη διασφάλισης της εναρμονισμένης εφαρμογής της οδηγίας σε πολλούς διαφορετικούς τομείς, προστατεύοντας παράλληλα την ιδιαιτερότητα κάθε τομέα χωριστά, σημαντική κρίνεται επίσης η συμμετοχή ενδιαφερομένων από διάφορους τομείς.

Τρίτο βήμα - **Ανάπτυξη πλαισίου διακυβέρνησης**

Για να είναι αποδοτικό και αποτελεσματικό, το πλαίσιο διακυβέρνησης θα πρέπει να στηρίζεται σε βασικούς ενδιαφερομένους, σε προτεραιότητες που έχουν καθοριστεί κατά τη διαδικασία σύνταξης, καθώς και στους περιορισμούς και στο πλαίσιο των εθνικών διοικητικών και πολιτικών δομών. Θα ήταν επιθυμητό να προβλεφθεί η απευθείας υποβολή εκθέσεων σε πολιτικό επίπεδο, ήτοι το πλαίσιο να διαθέτει δυνατότητα λήψης αποφάσεων και κατανομής πόρων, καθώς και η υποβολή συνεισφορών από ειδικούς σε θέματα ασφάλειας στον κυβερνοχώρο και παράγοντες της βιομηχανίας. Στο άρθρο 7 παράγραφος 1 στοιχείο β) της οδηγίας ΑΔΠ γίνεται ειδική αναφορά στο πλαίσιο διακυβέρνησης, συμπεριλαμβανομένων *«των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων»*.

Τέταρτο βήμα - **Τελική σύνθεση και επανεξέταση του σχεδίου στρατηγικής**

Στο στάδιο αυτό θα πρέπει να γίνει η τελική σύνθεση και επανεξέταση του σχεδίου στρατηγικής με τη διενέργεια ανάλυσης των πλεονεκτημάτων, αδυναμιών, ευκαιριών και απειλών (ΠΑΕΑ), μέσω της οποίας μπορεί να προσδιοριστεί αν απαιτείται αναθεώρηση του περιεχομένου. Μετά την εσωτερική επανεξέταση, θα πρέπει να διεξαχθεί η διαβούλευση με τους ενδιαφερομένους. Σημαντικό θα ήταν επίσης να οργανωθεί δημόσια διαβούλευση προκειμένου να επισημανθεί στο ευρύ κοινό η σημασία της προτεινόμενης στρατηγικής, να ληφθεί ανατροφοδότηση από όλες τις πιθανές πηγές και να αναζητηθεί στήριξη για την εξεύρεση των πόρων που απαιτούνται για την επακόλουθη εφαρμογή της στρατηγικής.

Πέμπτο βήμα – **Επίσημη έγκριση**

Το τελευταίο αυτό στάδιο περιλαμβάνει την επίσημη έγκριση της στρατηγικής σε πολιτικό επίπεδο από κοινού με έναν υποστηρικτικό προϋπολογισμό ο οποίος θα αντικατοπτρίζει τη σοβαρότητα που αποδίδει το εκάστοτε κράτος μέλος στο ζήτημα της ασφάλειας στον κυβερνοχώρο. Για την επίτευξη των στόχων της οδηγίας ΑΔΠ και στο πλαίσιο της κοινοποίησης του εγγράφου εθνικής στρατηγικής στην Επιτροπή σύμφωνα με το άρθρο 7 παράγραφος 3, η Επιτροπή ενθαρρύνει τα κράτη μέλη να υποβάλουν πληροφορίες για τον συναφή προϋπολογισμό. Η ανάληψη δεσμεύσεων σχετικά με τον προϋπολογισμό και τους απαιτούμενους ανθρώπινους πόρους είναι εξαιρετικά κρίσιμη για την αποτελεσματική εφαρμογή της στρατηγικής και της οδηγίας. Δεδομένου ότι η ασφάλεια στον κυβερνοχώρο είναι ακόμη ένας μάλλον νέος και ταχέως αναπτυσσόμενος τομέας δημόσιας πολιτικής, στις περισσότερες περιπτώσεις απαιτούνται νέες επενδύσεις, παρά το γεγονός ότι η γενικότερη κατάσταση των δημόσιων οικονομικών επιβάλλει περικοπές και εξοικονομήσεις.

Συμβουλές για τη διαδικασία και το περιεχόμενο των εθνικών στρατηγικών παρέχονται από διάφορους δημόσιους και ακαδημαϊκούς φορείς όπως, π.χ., τον ENISA[6], τη Διεθνή Ένωση Τηλεπικοινωνιών (ΔΕΤ)[7], τον ΟΟΣΑ[8], το Παγκόσμιο Φόρουμ Εμπειρογνωμόνων για τον Κυβερνοχώρο και το Πανεπιστήμιο της Οξφόρδης[9].

[6] ENISA, *National Cyber-Security Strategy Good Practice* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ΔΕΤ, *National Cybersecurity Strategy Guide (Οδηγός ανάπτυξης εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο* (2011). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
Η ΔΕΤ θα δημοσιεύσει επίσης μέσα στο 2017 μια εργαλειοθήκη με θέμα την κατάρτιση εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο (βλ. παρουσίαση στον δικτυακό τόπο http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] ΟΟΣΑ, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies (Η χάραξη πολιτικής για την ασφάλεια στον κυβερνοχώρο σε σημείο καμπής: Ανάλυση της νέας γενιάς εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο)* (2012). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Παγκόσμιο Κέντρο Ικανοτήτων για την ασφάλεια στον κυβερνοχώρο και Πανεπιστήμιο της Οξφόρδης, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Αναθεωρημένη έκδοση* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

2.4. Συγκεκριμένες ενέργειες που πρέπει να κάνουν τα κράτη μέλη πριν από την εκπνοή της προθεσμίας μεταφοράς στο εθνικό δίκαιο

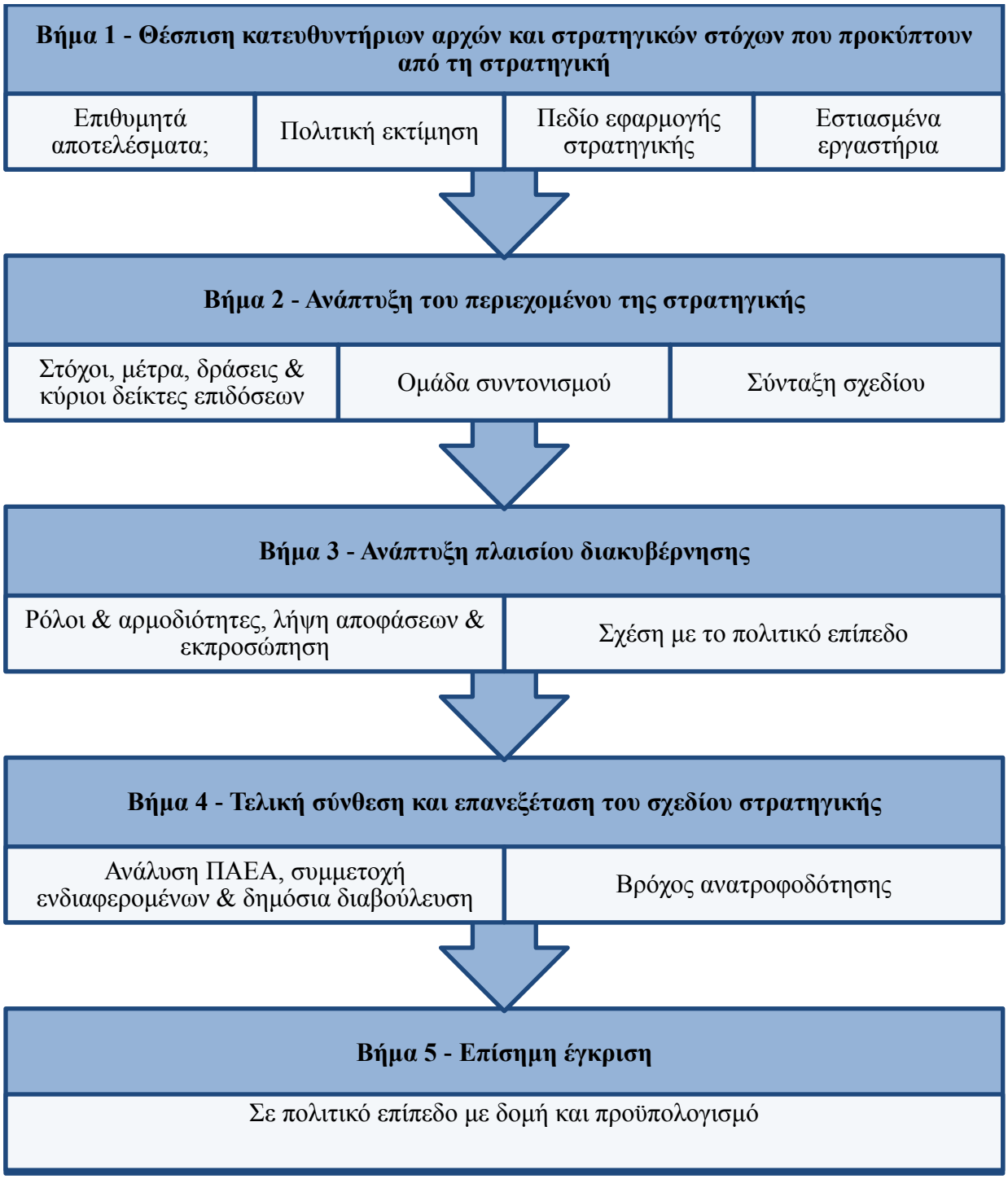
Σχεδόν όλα τα κράτη μέλη[10] είχαν δημοσιεύσει έγγραφα ΕΣΑΚ πριν από την έκδοση της οδηγίας. Στην ενότητα 6 του παρόντος παραρτήματος παρατίθενται οι στρατηγικές που ισχύουν επί του παρόντος σε κάθε κράτος μέλος[11], οι οποίες περιλαμβάνουν κατά κανόνα στρατηγικές αρχές, κατευθυντήριες γραμμές. στόχους, και σε ορισμένες περιπτώσεις ειδικά μέτρα για τον μετριασμό των κινδύνων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

Δεδομένου ότι ορισμένες από αυτές τις στρατηγικές υιοθετήθηκαν πριν από την έκδοση της οδηγίας ΑΔΠ, είναι πιθανό να μην περιέχουν απαραιτήτως όλα τα στοιχεία του άρθρου 7. Για να διασφαλιστεί η ορθή μεταφορά της οδηγίας στο εθνικό δίκαιο, τα κράτη μέλη θα πρέπει να προβούν σε ανάλυση των ελλείψεων και να συγκρίνουν το περιεχόμενο των ΕΣΑΚ τους με τις επτά διακριτές απαιτήσεις του άρθρου 7 για όλους τους τομείς που αναφέρονται στο παράρτημα ΙΙ και για όλες τις υπηρεσίες που περιλαμβάνονται στο παράρτημα ΙΙΙ της οδηγίας. Ακολούθως, θα πρέπει να προβούν στην κάλυψη των ελλείψεων που θα εντοπίσουν είτε επανεξετάζοντας τις ΕΣΑΚ που ήδη διαθέτουν, είτε προβαίνοντας σε πλήρη αναθεώρηση των αρχών στις οποίες βασίζονται οι εθνικές στρατηγικές τους για την ασφάλεια δικτύων και πληροφοριών. Οι κατευθυντήριες γραμμές που παρατίθενται ανωτέρω σχετικά με τη διαδικασία έγκρισης ΕΣΑΚ ισχύουν και για την επανεξέταση και επικαιροποίηση των ΕΣΑΚ που ήδη υπάρχουν.

[10] Με εξαίρεση την Ελλάδα, όπου η εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο βρίσκεται στο στάδιο της κατάρτισης από το 2014 (βλ. δικτυακό τόπο https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Οι συγκεκριμένες πληροφορίες βασίζονται στην επισκόπηση των ΕΣΑΚ που εκπόνησε ο ENISA, η οποία είναι διαθέσιμη στον δικτυακό τόπο https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Σχήμα 1: Διαδικασία πέντε βημάτων για την έγκριση ΕΣΑΚ



3. Οδηγία ΑΔΠ: Εθνικές αρμόδιες αρχές, ενιαία κέντρα επαφής και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT).

Σύμφωνα με το άρθρο 8 παράγραφος 1, τα κράτη μέλη οφείλουν να ορίσουν μία ή περισσότερες εθνικές αρμόδιες αρχές, που θα καλύπτουν τουλάχιστον τους τομείς που αναφέρονται στο παράρτημα ΙΙ και τις υπηρεσίες που αναφέρονται στο παράρτημα ΙΙΙ της

οδηγίας, με καθήκον να παρακολουθούν την εφαρμογή της οδηγίας. Τα κράτη μέλη μπορούν να αναθέτουν το ρόλο αυτόν σε υφιστάμενη αρχή ή αρχές.

Η παρούσα ενότητα δίνει έμφαση στους τρόπους με τους οποίους η οδηγία ΑΔΠ ενισχύει την ετοιμότητα των κρατών μελών απαιτώντας από τα τελευταία να συστήσουν αποτελεσματικές εθνικές αρμόδιες αρχές και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT). Πιο συγκεκριμένα, η παρούσα ενότητα καλύπτει την υποχρέωση του ορισμού εθνικών αρμόδιων αρχών, περιλαμβανομένου του ρόλου του ενιαίου κέντρου επαφής. Εξετάζει δε τρία ζητήματα: α) τις πιθανές εθνικές δομές διακυβέρνησης (π.χ. πρότυπα κεντρικής, αποκεντρωμένης διακυβέρνησης κ.λπ.) και λοιπές απαιτήσεις· β) τον ρόλο του ενιαίου κέντρου επαφής και γ) τις ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών.

3.1. Είδη αρχών

Το άρθρο 8 της οδηγίας ΑΔΠ επιβάλλει στα κράτη μέλη την υποχρέωση να ορίσουν εθνικές αρμόδιες αρχές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, αναγνωρίζοντας ρητώς τη δυνατότητά τους να ορίσουν *«μία ή περισσότερες εθνικές αρμόδιες αρχές»*. Η αιτιολογική σκέψη 30 της οδηγίας επεξηγεί τη συγκεκριμένη επιλογή πολιτικής: «*Με δεδομένες τις διαφορές των εθνικών δομών διακυβέρνησης και προκειμένου να διασφαλιστούν οι ήδη υφιστάμενες τομεακές ρυθμίσεις ή οι εποπτικοί και ρυθμιστικοί φορείς της Ένωσης, καθώς και προς αποφυγή αλληλοεπικαλύψεων, τα κράτη μέλη θα πρέπει να είναι σε θέση να ορίζουν περισσότερες από μία αρμόδιες εθνικές αρχές για την εκτέλεση των καθηκόντων που συνδέονται με την ασφάλεια των συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών δυνάμει της παρούσας οδηγίας».*

Συνεπώς, τα κράτη μέλη είναι ελεύθερα να επιλέξουν εάν θα ορίσουν μία κεντρική αρχή η οποία θα είναι αρμόδια για όλους τους τομείς και τις υπηρεσίες που καλύπτονται από την οδηγία ή περισσότερες αρχές, ανάλογα π.χ. με το είδος του εκάστοτε τομέα.

Αφού αποφασίσουν ποια προσέγγιση θα υιοθετήσουν, τα κράτη μέλη μπορούν να βασιστούν στην πείρα που έχει αποκτηθεί από τις εθνικές προσεγγίσεις που χρησιμοποιήθηκαν στο πλαίσιο της υφιστάμενης νομοθεσίας για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας. Όπως περιγράφεται στον πίνακα 1, στην περίπτωση της προστασίας των υποδομών πληροφοριών ζωτικής σημασίας, τα κράτη μέλη αποφάσισαν να υιοθετήσουν είτε κεντρική είτε αποκεντρωμένη προσέγγιση όσον αφορά την κατανομή αρμοδιοτήτων σε εθνικό επίπεδο. Τα παραδείγματα των χωρών που παρατίθενται ακολούθως εξυπηρετούν αποκλειστικά σκοπούς πληροφόρησης. Στόχος είναι να ενημερωθούν τα κράτη μέλη για τα οργανωτικά πλαίσια που ήδη υπάρχουν. Η Επιτροπή δεν υπονοεί επομένως σε καμία περίπτωση ότι τα μοντέλα που χρησιμοποίησαν κάποιες χώρες για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας θα πρέπει να χρησιμοποιηθούν απαραιτήτως για τον σκοπό της μεταφοράς στο εθνικό δίκαιο της οδηγίας ΑΔΠ.

Κάθε κράτος μέλος μπορεί κάλλιστα να επιλέξει τον δικό του συνδυασμό ρυθμίσεων που να περιλαμβάνει στοιχεία τόσο της κεντρικής όσο και της αποκεντρωμένης προσέγγισης. Οι εν

λόγω επιλογές μπορούν να γίνουν με βάση προγενέστερες εθνικές ρυθμίσεις διακυβέρνησης για τους διάφορους τομείς και υπηρεσίες που καλύπτονται από την οδηγία, ή με βάση ρυθμίσεις που θεσπίζονται για πρώτη φορά από τις εμπλεκόμενες αρχές και από τους οικείους ενδιαφερομένους που έχουν προσδιοριστεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών και πάροχοι ψηφιακών υπηρεσιών. Σημαντικές παράμετροι που θα καθορίσουν τις τελικές επιλογές των κρατών μελών είναι επίσης η ύπαρξη εξειδικευμένων γνώσεων για την ασφάλεια στον κυβερνοχώρο, τα συναφή με την εξεύρεση πόρων ζητήματα, καθώς και οι σχέσεις ανάμεσα στους ενδιαφερομένους και τα εθνικά συμφέροντα (για παράδειγμα, οικονομική ανάπτυξη, δημόσια ασφάλεια κ.λπ.).

3.2 Δημοσιότητα και πρόσθετες σχετικές πτυχές

Σύμφωνα με το άρθρο 8 παράγραφος 7, τα κράτη μέλη οφείλουν να ενημερώσουν την Επιτροπή για τον ορισμό των εθνικών αρμόδιων αρχών και για τα καθήκοντα των τελευταίων πριν από την εκπνοή της προθεσμίας μεταφοράς.

Τα άρθρα 15 και 17 της οδηγίας ΑΔΠ επιβάλλουν στα κράτη μέλη την υποχρέωση να διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν τις αναγκαίες εξουσίες και μέσα για να εκτελούν τα καθήκοντα που προβλέπονται στα εν λόγω άρθρα.

Υποχρεωτική είναι επίσης η δημοσιοποίηση του ορισμού συγκεκριμένων οντοτήτων ως εθνικών αρμόδιων αρχών. Η οδηγία δεν ορίζει τον τρόπο με τον οποίον πρέπει να γίνεται η εν λόγω δημοσιοποίηση. Δεδομένου ότι ο στόχος της συγκεκριμένης απαίτησης είναι να εξασφαλιστεί η καλύτερη δυνατή ενημέρωση των παραγόντων που καλύπτονται από την οδηγία ΑΔΠ και του ευρύτερου κοινού, και με βάση τις εμπειρίες από άλλους τομείς (τηλεπικοινωνίες, τράπεζες, φαρμακευτικός κλάδος), η Επιτροπή εκτιμά ότι αυτό θα μπορούσε να επιτευχθεί, π.χ., μέσω μιας ευρέως προβεβλημένης διαδικτυακής πύλης.

Το άρθρο 8 παράγραφος 5 της οδηγίας ΑΔΠ επιβάλλει την υποχρέωση στις εν λόγω αρχές να διαθέτουν «επαρκείς πόρους» για να επιτελούν τα καθήκοντα που τους ανατίθενται δυνάμει της οδηγίας.

Πίνακας 1: Εθνικές προσεγγίσεις για την προστασία υποδομών πληροφοριών ζωτικής σημασίας (CIIP).

Το 2016, ο ENISA δημοσίευσε μελέτη[12] με θέμα τις διάφορες προσεγγίσεις που ακολουθούν τα κράτη μέλη για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας που διαθέτουν. Ακολούθως περιγράφονται δύο διαφορετικά προφίλ διακυβέρνησης που ακολουθούν τα κράτη μέλη στον τομέα της προστασίας υποδομών πληροφοριών ζωτικής σημασίας, τα οποία μπορούν να χρησιμοποιηθούν στο πλαίσιο της μεταφοράς της οδηγίας ΑΔΠ στα εθνικά δίκαια.

Προφίλ 1: Αποκεντρωμένη προσέγγιση: διάφορες αρχές ανά τομέα είναι αρμόδιες για συγκεκριμένους τομείς και υπηρεσίες που αναφέρονται στα παραρτήματα ΙΙ και ΙΙΙ της οδηγίας.

Η αποκεντρωμένη προσέγγιση χαρακτηρίζεται από:

(i) την αρχή της επικουρικότητας
(ii) τη στενή συνεργασία μεταξύ των δημόσιων οργανισμών
(iii)την τομεακή νομοθεσία

Η αρχή της επικουρικότητας.

Αντί της θέσπισης ή του ορισμού ενιαίου οργανισμού που φέρει τη γενική ευθύνη, η αποκεντρωμένη προσέγγιση ακολουθεί την αρχή της επικουρικότητας. Αυτό σημαίνει ότι η ευθύνη της εφαρμογής εμπίπτει στην αρμοδιότητα μιας τομεακής αρχής, η οποία κατανοεί καλύτερα από κάθε άλλον τον τοπικό τομέα και έχει ήδη εδραιωμένη σχέση με τους ενδιαφερομένους. Δυνάμει της εν λόγω αρχής, οι αποφάσεις λαμβάνονται από όσους βρίσκονται πλησιέστερα σε εκείνους που επηρεάζονται.

Στενή συνεργασία μεταξύ των δημόσιων οργανισμών

Λόγω της πληθώρας και της ποικιλομορφίας των δημόσιων οργανισμών που εμπλέκονται στην προστασία των υποδομών πληροφοριών ζωτικής σημασίας, πολλά κράτη μέλη έχουν αναπτύξει διάφορα συστήματα συνεργασίας για τον συντονισμό των εργασιών και των προσπαθειών των διαφόρων αρχών, από άτυπα δίκτυα μέχρι περισσότερο θεσμοθετημένες πλατφόρμες συζήτησης ή ρυθμίσεις. Τα εν λόγω συστήματα συνεργασίας, πάντως, εξυπηρετούν μόνο τον σκοπό της ανταλλαγής πληροφοριών και του συντονισμού μεταξύ των διαφόρων δημόσιων οργανισμών, χωρίς να έχουν οποιαδήποτε εξουσία επάνω τους.

Τομεακή νομοθεσία

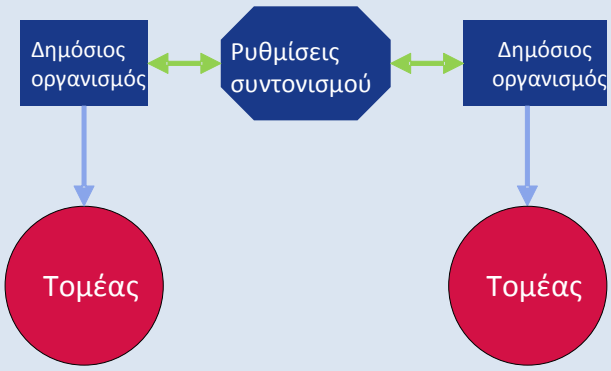
Οι χώρες που ακολουθούν την αποκεντρωμένη προσέγγιση στους διάφορους τομείς ζωτικής σημασίας αποφεύγουν συχνά να νομοθετήσουν σε κεντρικό επίπεδο για θέματα που άπτονται της προστασίας υποδομών πληροφοριών ζωτικής σημασίας. Αντ' αυτού, εξακολουθούν να επιλέγουν την έκδοση νόμων και κανονισμών ανά τομέα με αποτέλεσμα να υπάρχουν

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs (Απολογισμός, ανάλυση και συστάσεις για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας)* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

σημαντικές αποκλίσεις μεταξύ των διαφόρων τομέων. Η συγκεκριμένη προσέγγιση παρουσιάζει το πλεονέκτημα της ευθυγράμμισης των μέτρων που σχετίζονται με την ΑΔΠ με τους ήδη ισχύοντες κανονισμούς ανά τομέα με γνώμονα τη βελτίωση τόσο της αποδοχής από τον τομέα όσο και της αποτελεσματικότητας της επιβολής από την οικεία αρχή.

Η εφαρμογή αμιγώς αποκεντρωμένης προσέγγισης εγκυμονεί όμως σοβαρό κίνδυνο μειωμένης συνοχής κατά την εφαρμογή της οδηγίας στους διάφορους τομείς και υπηρεσίες. Στην περίπτωση αυτή, η οδηγία προβλέπει την ύπαρξη εθνικού ενιαίου κέντρου επαφής το οποίο θα ασκεί καθήκοντα συνδέσμου για διασυνοριακά ζητήματα. Η εν λόγω οντότητα θα μπορούσε επιπλέον να επιφορτιστεί από το οικείο κράτος μέλος με τα καθήκοντα του εσωτερικού συντονισμού και της συνεργασίας μεταξύ των διαφόρων εθνικών αρμόδιων αρχών, σύμφωνα με το άρθρο 10 της οδηγίας.

Σχήμα 2 – Αποκεντρωμένη προσέγγιση



Παραδείγματα αποκεντρωμένης προσέγγισης

Η Σουηδία αποτελεί καλό παράδειγμα χώρας που ακολουθεί αποκεντρωμένη προσέγγιση στον τομέα της προστασίας των υποδομών πληροφοριών ζωτικής σημασίας. Η χώρα χρησιμοποιεί την προσέγγιση της «προοπτικής συστήματος». Αυτό σημαίνει ουσιαστικά ότι τα βασικά καθήκοντα της προστασίας των υποδομών πληροφοριών ζωτικής σημασίας, όπως ο προσδιορισμός υπηρεσιών και υποδομών ζωτικής σημασίας, ο συντονισμός και η στήριξη των φορέων εκμετάλλευσης, τα ρυθμιστικά καθήκοντα, καθώς και τα μέτρα ετοιμότητας σε περιπτώσεις έκτακτης ανάγκης, ανήκουν στην αρμοδιότητα διαφόρων οργανισμών και δήμων. Μεταξύ των εν λόγω οργανισμών συγκαταλέγονται ο σουηδικός Οργανισμός Πολιτικής Προστασίας (MSB), ο σουηδικός Οργανισμός Ταχυδρομείων και Τηλεπικοινωνιών (PTS), και διάφοροι σουηδικοί οργανισμοί που δραστηριοποιούνται στους τομείς της άμυνας, του στρατού και της επιβολής του νόμου.

Για τον συντονισμό των δράσεων μεταξύ των διαφόρων οργανισμών και δημόσιων οντοτήτων, η σουηδική κυβέρνηση έχει αναπτύξει ένα δίκτυο συνεργασίας το οποίο αποτελείται από αρχές «με συγκεκριμένες αρμοδιότητες έναντι της κοινωνίας στον τομέα της ασφάλειας των

πληροφοριών». Η εν λόγω ομάδα συνεργασίας για την ασφάλεια των πληροφοριών (SAMFI) αποτελείται από εκπροσώπους των διαφόρων αρχών και συνέρχεται αρκετές φορές ετησίως για να συζητήσει ζητήματα που σχετίζονται με την ασφάλεια των πληροφοριών σε εθνικό επίπεδο. Τα θέματα με τα οποία ασχολείται η SAMFI προέρχονται ως επί το πλείστον από πολιτικο-στρατηγικούς τομείς και καλύπτουν πτυχές όπως τα τεχνικά ζητήματα και η τυποποίηση, η εθνική και διεθνής ανάπτυξη στον τομέα της ασφάλειας των πληροφοριών ή η διαχείριση και η πρόληψη συμβάντων στον τομέα των τεχνολογιών πληροφοριών. (Οργανισμός Πολιτικής Προστασίας (MSB) της Σουηδίας, 2015).

Η Σουηδία δεν έχει εκδώσει κεντρική νομοθεσία για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας, η οποία να ισχύει για τους φορείς εκμετάλλευσης υποδομών πληροφοριών ζωτικής σημασίας όλων των τομέων. Αντ' αυτού, η ψήφιση νομοθεσίας με υποχρεώσεις για τις εταιρείες που δραστηριοποιούνται σε συγκεκριμένους τομείς εμπίπτει στην αρμοδιότητα των αντίστοιχων δημόσιων αρχών. Για παράδειγμα, ο MSB έχει το δικαίωμα να εκδίδει κανονισμούς για κρατικές αρχές στον τομέα της ασφάλειας των πληροφοριών, ενώ ο PTS μπορεί να επιβάλλει στους φορείς εκμετάλλευσης να εφαρμόζουν ορισμένα τεχνικά ή οργανωτικά μέτρα ασφάλειας που απορρέουν από παράγωγο δίκαιο.

Άλλο παράδειγμα χώρας που παρουσιάζει χαρακτηριστικά αυτού του προφίλ διακυβέρνησης είναι η Ιρλανδία, η οποία ακολουθεί το «δόγμα της επικουρικότητας», δηλαδή κάθε υπουργείο είναι υπεύθυνο για τον προσδιορισμό υποδομών πληροφοριών ζωτικής σημασίας και την εκτίμηση κινδύνου για τον δικό του τομέα. Επιπλέον, δεν έχουν θεσπιστεί ειδικοί κανονισμοί για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας σε εθνικό επίπεδο. Η νομοθεσία εξακολουθεί να έχει τομεακό χαρακτήρα και υφίσταται κατά κύριο λόγο για τον τομέα της ενέργειας και των τηλεπικοινωνιών (2015). Άλλα παραδείγματα είναι η Αυστρία, η Κύπρος και η Φινλανδία.

Προφίλ 2: Κεντρική προσέγγιση: μία κεντρική αρχή είναι αρμόδια για όλους τους τομείς και τις υπηρεσίες που αναφέρονται στα παραρτήματα II και III της οδηγίας.

Η κεντρική προσέγγιση χαρακτηρίζεται από:

i) μία κεντρική αρχή για όλους τους τομείς
ii) Ολοκληρωμένο νομοθετικό πλαίσιο

Μία κεντρική αρχή για όλους τους τομείς

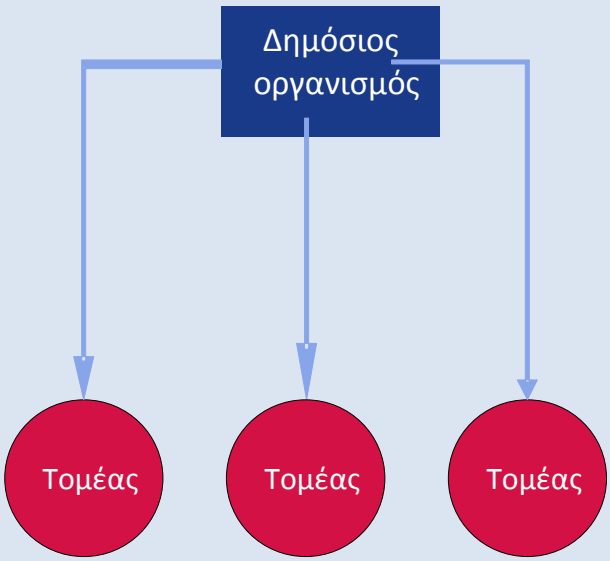
Τα κράτη μέλη που ακολουθούν κεντρική προσέγγιση έχουν συστήσει αρχές με ευθύνες και ευρείες αρμοδιότητες σε πολλούς ή σε όλους τους τομείς ζωτικής σημασίας, ή έχουν επεκτείνει τις εξουσίες των υφιστάμενων αρχών. Οι βασικές αυτές αρχές, που είναι αρμόδιες για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας, επιτελούν συνδυαστικά διάφορα καθήκοντα, όπως σχεδιασμό αντιμετώπισης απρόοπτων καταστάσεων, διαχείριση καταστάσεων έκτακτης ανάγκης, ρυθμιστικά καθήκοντα και παροχή στήριξης σε ιδιωτικούς φορείς εκμετάλλευσης. Σε πολλές περιπτώσεις, η εθνική ή κρατική CSIRT υπάγεται στη βασική αρχή προστασίας υποδομών πληροφοριών ζωτικής σημασίας. Η κεντρική αρχή είναι πιθανό να διαθέτει περισσότερη εμπειρογνωσία σε θέματα ασφάλειας στον κυβερνοχώρο από

τις διάφορες τομεακές αρχές, δεδομένης της γενικότερης έλλειψης δεξιοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο.

Ολοκληρωμένο νομοθετικό πλαίσιο

Η ύπαρξη ολοκληρωμένου νομοθετικού πλαισίου δημιουργεί υποχρεώσεις και απαιτήσεις για όλους τους φορείς εκμετάλλευσης υποδομών πληροφοριών ζωτικής σημασίας ανεξαρτήτως τομέα. Ολοκληρωμένο νομοθετικό πλαίσιο μπορεί να επιτευχθεί είτε με την έγκριση νέων ολοκληρωμένων νομοθετικών πράξεων είτε με τη συμπλήρωση των ήδη υφιστάμενων κανονισμών ανά τομέα. Η προσέγγιση αυτή αναμένεται να διευκολύνει τη συνεκτική εφαρμογή της οδηγίας ΑΔΠ σε όλους τους τομείς και τις υπηρεσίες που καλύπτονται από αυτήν. Αναμένεται ακόμη να αποτρέψει τον κίνδυνο της εμφάνισης κενών κατά την εφαρμογή που είναι υπαρκτός όταν υπάρχουν πολλές αρχές με συγκεκριμένες αρμοδιότητες.

Σχήμα 3 – Κεντρική προσέγγιση



Παραδείγματα κεντρικής προσέγγισης

Η Γαλλία είναι καλό παράδειγμα κράτους μέλους της ΕΕ που ακολουθεί κεντρική προσέγγιση. Ο γαλλικός εθνικός οργανισμός για την ασφάλεια των συστημάτων πληροφοριών (Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI) ορίστηκε το 2011 ως η βασική εθνική αρχή για την προστασία των συστημάτων πληροφοριών. Ο ANSSI είναι επιφορτισμένος με την εποπτεία των «φορέων εκμετάλλευσης ζωτικής σημασίας» (OIV): μπορεί να επιβάλει στους OIV να συμμορφώνονται με μέτρα ασφαλείας και είναι εξουσιοδοτημένος να διενεργεί ελέγχους ασφαλείας σε αυτούς. Επιπλέον, είναι το κύριο ενιαίο κέντρο επαφής για τους OIV, οι οποίοι υποχρεούνται να γνωστοποιούν στον ANSSI τυχόν συμβάντα ασφαλείας.

Σε περίπτωση συμβάντων ασφαλείας, ο ANSSI ενεργεί ως οργανισμός αντιμετώπισης απρόοπτων καταστάσεων στον τομέα της προστασίας των υποδομών πληροφοριών ζωτικής σημασίας και αποφασίζει τα μέτρα που πρέπει να λάβουν οι φορείς εκμετάλλευσης για την αντιμετώπιση της κρίσης. Ο συντονισμός των ενεργειών της κυβέρνησης γίνεται στο κέντρο επιχειρήσεων του ANSSI. Ο εντοπισμός των απειλών και η αντιμετώπιση των συμβάντων σε επιχειρησιακό επίπεδο γίνεται από τη γαλλική ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-FR), η οποία υπάγεται στον ANSSI.

Η Γαλλία έχει θεσπίσει ολοκληρωμένο νομοθετικό πλαίσιο για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας. Το 2006, ο πρωθυπουργός διέταξε να συνταχθεί κατάλογος με τους τομείς υποδομών ζωτικής σημασίας. Με βάση τον συγκεκριμένο κατάλογο, στον οποίον συμπεριλήφθηκαν δώδεκα τομείς ζωτικής σημασίας, η κυβέρνηση όρισε περίπου 250 OIV. Το 2013 ψηφίστηκε ο νόμος περί στρατιωτικού προγραμματισμού (LPM)[13], ο οποίος θεσπίζει διάφορες υποχρεώσεις για τους OIV, όπως αναφορά συμβάντων ή εφαρμογή μέτρων ασφαλείας. Οι απαιτήσεις αυτές είναι υποχρεωτικές για όλους τους OIV όλων των τομέων (Γερουσία της Γαλλίας, 2013).

3.3. Οδηγία ΑΔΠ, άρθρο 9: Ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT).

Σύμφωνα με το άρθρο 9, τα κράτη μέλη οφείλουν να ορίσουν μία ή περισσότερες CSIRT οι οποίες θα είναι υπεύθυνες για τον χειρισμό κινδύνων και συμβάντων που σχετίζονται με τους τομείς και τις υπηρεσίες που αναφέρονται στα παραρτήματα ΙΙ και ΙΙΙ της οδηγίας. Λαμβάνοντας υπόψη την απαίτηση της ελάχιστης εναρμόνισης που προβλέπεται στο άρθρο 3 της οδηγίας, τα κράτη μέλη είναι ελεύθερα να χρησιμοποιούν τις CSIRT και για άλλους τομείς που δεν καλύπτονται από την οδηγία, όπως οι φορείς δημόσιας διοίκησης.

[13] La loi de programmation militaire

Τα κράτη μέλη μπορούν να επιλέξουν να συγκροτήσουν τη CSIRT στους κόλπους της αρμόδιας εθνικής αρχής[14].

3.4. Καθήκοντα και απαιτήσεις

Στα καθήκοντα των CSIRT που θα οριστούν, τα οποία προβλέπονται στο παράρτημα Ι της οδηγίας ΑΔΠ, περιλαμβάνονται, μεταξύ άλλων, τα εξής:

- παρακολούθηση συμβάντων σε εθνικό επίπεδο·
- παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων επαγρύπνησης καθώς και ανακοινώσεων και διάδοση πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα·
- παρέμβαση σε περίπτωση συμβάντος·
- παροχή δυναμικής ανάλυσης κινδύνων και συμβάντων και επίγνωση της κατάστασης· και
- συμμετοχή στο δίκτυο των εθνικών CSIRT (δίκτυο CSIRT) που θεσπίζεται δυνάμει του άρθρου 12.

Το άρθρο 14 παράγραφοι 3, 5 και 6 και το άρθρο 16 παράγραφοι 3, 6 και 7 προβλέπουν συγκεκριμένα πρόσθετα καθήκοντα σε σχέση με τις κοινοποιήσεις συμβάντων όταν ένα κράτος μέλος αποφασίζει ότι οι CSIRT είναι σε θέση να αναλάβουν τέτοιους ρόλους επιπλέον ή αντί των εθνικών αρμόδιων αρχών.

Στο πλαίσιο της μεταφοράς της οδηγίας στο εθνικό δίκαιο, τα κράτη μέλη διαθέτουν διάφορες επιλογές όσον αφορά τον ρόλο των CSIRT σε σχέση με τις απαιτήσεις κοινοποίησης συμβάντων. Είναι δυνατή καταρχάς η απευθείας υποχρεωτική υποβολή εκθέσεων στις CSIRT, η οποία έχει το πλεονέκτημα της διοικητικής αποτελεσματικότητας. Εναλλακτικά, τα κράτη μέλη μπορούν να επιλέξουν απευθείας υποβολή εκθέσεων στις εθνικές αρμόδιες αρχές με δικαίωμα πρόσβασης των CSIRT στις πληροφορίες που υποβάλλονται. Απώτερη επιδίωξη των CSIRT είναι η επίλυση προβλημάτων που σχετίζονται με την αποτροπή, τον εντοπισμό, την αντιμετώπιση και τον μετριασμό του αντίκτυπου συμβάντων στον κυβερνοχώρο (περιλαμβανομένων των συμβάντων που δεν είναι ζωτικής σημασίας για να αποτελέσουν αντικείμενο υποχρεωτικής αναφοράς) από κοινού με τους οικείους ενδιαφερομένους, ενώ η συμμόρφωση με τις κανονιστικές ρυθμίσεις εμπίπτει στην αρμοδιότητα των εθνικών αρμόδιων αρχών.

Σύμφωνα με το άρθρο 9 παράγραφος 3 της οδηγίας, τα κράτη μέλη οφείλουν επίσης να μεριμνούν ώστε οι CSIRT τους να έχουν πρόσβαση σε ασφαλή και ανθεκτική υποδομή ΤΠΕ.

Το άρθρο 9 παράγραφος 4 της οδηγίας επιβάλλει στα κράτη μέλη την υποχρέωση να ενημερώνουν την Επιτροπή σχετικά με την εντολή καθώς και σχετικά με τα βασικά στοιχεία της διαδικασίας χειρισμού συμβάντων από τις ορισθείσες CSIRT.

[14] Βλ. άρθρο 9 παράγραφος 1 τελευταία πρόταση.

Οι απαιτήσεις των CSIRT που ορίζονται από τα κράτη μέλη παρατίθενται στο παράρτημα Ι της οδηγίας ΑΔΠ. Οι CSIRT πρέπει να εξασφαλίζουν υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών τους. Τα γραφεία τους και τα υποστηρικτικά συστήματα πληροφοριών πρέπει να εγκαθίστανται σε ασφαλείς χώρους και να διασφαλίζουν την αδιάλειπτη λειτουργία τους. Επιπλέον, οι CSIRT θα πρέπει να έχουν τη δυνατότητα να συμμετέχουν σε διεθνή δίκτυα συνεργασίας.

3.5. Παροχή συνδρομής για την ανάπτυξη των CSIRT

Μέσω του προγράμματος υποδομών ψηφιακών υπηρεσιών (ΥΨΥ) για την ασφάλεια στον κυβερνοχώρο του χρηματοδοτικού μηχανισμού «Συνδέοντας την Ευρώπη» είναι δυνατό να διατεθεί σημαντική ενωσιακή χρηματοδότηση για την παροχή συνδρομής στις CSIRT των κρατών μελών με στόχο τη βελτίωση των ικανοτήτων τους και της μεταξύ τους συνεργασίας μέσω ενός μηχανισμού συνεργασίας και ανταλλαγής πληροφοριών. Σκοπός του μηχανισμού συνεργασίας που αναπτύσσεται επί του παρόντος στο πλαίσιο του έργου SMART 2015/1089 είναι να διευκολύνει την ταχεία και αποτελεσματική επιχειρησιακή συνεργασία σε εθελοντική βάση μεταξύ των CSIRT των κρατών μελών, με γνώμονα ιδίως τη στήριξη των καθηκόντων με τα οποία επιφορτίζεται το δίκτυο CSIRT δυνάμει του άρθρου 12 της οδηγίας.

Αναλυτικότερες πληροφορίες σχετικά με τις προσκλήσεις υποβολής προτάσεων για την ανάπτυξη των ικανοτήτων των CSIRT των κρατών μελών διατίθενται μέσω του δικτυακού τόπου του Εκτελεστικού Οργανισμού Καινοτομίας και Δικτύων (INEA) της Ευρωπαϊκής Επιτροπής[15].

Ο φορέας διακυβέρνησης ΥΨΥ για την ασφάλεια στον κυβερνοχώρο του χρηματοδοτικού μηχανισμού «Συνδέοντας την Ευρώπη» συνιστά άτυπη δομή για την παροχή καθοδήγησης και συνδρομής σε επίπεδο πολιτικής στις CSIRT των κρατών μελών για τον σκοπό της ανάπτυξης ικανοτήτων και για την εφαρμογή του μηχανισμού εθελοντικής συνεργασίας.

Οι νεοσυσταθείσες CSIRT ή εκείνες που ορίζονται για την εκτέλεση των καθηκόντων που προβλέπονται στο παράρτημα Ι της οδηγίας ΑΔΠ μπορούν να βασιστούν στις συμβουλές και την εμπειρογνωσία του ENISA για να βελτιώσουν τις επιδόσεις τους και να φέρουν αποτελεσματικά εις πέρας το έργο τους[16]. Αξίζει δε να σημειωθεί στο σημείο αυτό ότι οι CSIRT των κρατών μελών θα μπορούσαν να έχουν ως σημείο αναφοράς κάποια από τα έργα που έχει εκπονήσει πρόσφατα ο ENISA. Συγκεκριμένα, όπως αναφέρεται στην ενότητα 7 του παρόντος παραρτήματος, ο ENISA έχει εκδώσει διάφορα έγγραφα και μελέτες σχετικά με ορθές πρακτικές και συστάσεις σε τεχνικό επίπεδο, όπου περιλαμβάνονται και αξιολογήσεις του επιπέδου ωριμότητας των CSIRT, για διάφορες ικανότητες και υπηρεσίες των CSIRT. Πραγματοποιείται επίσης ανταλλαγή κατευθυντήριων γραμμών και βέλτιστων πρακτικών μεταξύ δικτύων CSIRT τόσο σε παγκόσμιο (FIRST[17]) όσο και σε ευρωπαϊκό επίπεδο (Trusted Introducer, TI[18]).

[15] Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Βλ. άρθρο 9 παράγραφος 5 της οδηγίας ΑΔΠ.
[17] Φόρουμ ομάδων απόκρισης σε συμβάντα και ασφάλειας (https://www.first.org/)
[18] https://www.trusted-introducer.org/

3.6. Ο ρόλος του ενιαίου κέντρου επαφής.

Σύμφωνα με το άρθρο 8 παράγραφος 3 της οδηγίας ΑΔΠ, κάθε κράτος μέλος οφείλει να ορίσει ένα εθνικό ενιαίο κέντρο επαφής, το οποίο θα ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας με τις αρμόδιες αρχές άλλων κρατών μελών, καθώς και με την ομάδα συνεργασίας και το δίκτυο CSIRT[19] που θεσπίζονται δυνάμει της οδηγίας ΑΔΠ. Στην αιτιολογική σκέψη 31 και στο άρθρο 8 παράγραφος 4 εξηγείται η λογική στην οποία βασίζεται η εν λόγω απαίτηση, ήτοι η διευκόλυνση της διασυνοριακής συνεργασίας και επικοινωνίας. Τούτο είναι ιδιαίτερα αναγκαίο δεδομένου ότι τα κράτη μέλη μπορούν να αποφασίσουν να έχουν περισσότερες από μία εθνικές αρχές. Επομένως, η ύπαρξη ενιαίου κέντρου επαφής αναμένεται να διευκολύνει τον προσδιορισμό και τη συνεργασία αρχών από διάφορα κράτη μέλη.

Στα καθήκοντα συνδέσμου που θα ασκούν τα ενιαία κέντρα επαφής θα περιλαμβάνεται ενδεχομένως η επικοινωνία και η συνεργασία με τις γραμματείες της ομάδας συνεργασίας και του δικτύου CSIRT όταν το εθνικό ενιαίο κέντρο επαφής δεν είναι ούτε CSIRT ούτε μέλος της ομάδας συνεργασίας. Τα κράτη μέλη θα πρέπει να διασφαλίσουν επιπλέον ότι τα ενιαία κέντρα επαφής ενημερώνονται για τις κοινοποιήσεις που λαμβάνονται από φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών[20].

Το άρθρο 8 παράγραφος 3 της οδηγίας ορίζει ότι σε περίπτωση που κάποιο κράτος μέλος υιοθετήσει κεντρική προσέγγιση, ήτοι ορίσει μόνο μία αρμόδια αρχή, η εν λόγω αρχή θα έχει και ρόλο ενιαίου κέντρου επαφής. Αν κάποιο κράτος μέλος επιλέξει αποκεντρωμένη προσέγγιση, θα μπορεί να διαλέξει μία από τις διάφορες αρμόδιες αρχές και να της αναθέσει ρόλο ενιαίου κέντρου επαφής. Ανεξάρτητα από το θεσμικό πρότυπο που θα επιλεγεί, όταν η αρμόδια αρχή, η CSIRT και το ενιαίο κέντρο επαφής είναι διαφορετικές οντότητες, τα κράτη μέλη οφείλουν να διασφαλίζουν την μεταξύ τους αποτελεσματική συνεργασία με σκοπό την τήρηση των υποχρεώσεων που προβλέπονται στην παρούσα οδηγία[21].

Έως τις 9 Αυγούστου 2018, και στη συνέχεια κάθε έτος, το ενιαίο κέντρο επαφής οφείλει να υποβάλλει στην ομάδα συνεργασίας συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει, συμπεριλαμβανομένου του αριθμού των κοινοποιήσεων, της φύσης των συμβάντων και των μέτρων που έχουν ληφθεί από τις αρχές, όπως ενημέρωση άλλων επηρεαζόμενων κρατών μελών για το συμβάν ή παροχή συναφών πληροφοριών στην κοινοποιούσα εταιρεία για τον χειρισμό του συμβάντος[22]. Κατόπιν αιτήματος της αρμόδιας αρχής ή της CSIRT, το ενιαίο κέντρο επαφής οφείλει να διαβιβάζει τις κοινοποιήσεις των φορέων εκμετάλλευσης βασικών υπηρεσιών στα ενιαία κέντρα επαφής άλλων κρατών μελών που επηρεάζονται από τα συμβάντα[23].

[19] Δίκτυο εθνικών CSIRT για την προώθηση της επιχειρησιακής συνεργασίας ανάμεσα στα κράτη μέλη που δημιουργείται δυνάμει του άρθρου 12.
[20] Βλέπε άρθρο 10 παράγραφος 3
[21] Βλέπε άρθρο 10 παράγραφος 1
[22] Ό.π.
[23] Βλέπε άρθρο 14 παράγραφος 5

Τα κράτη μέλη οφείλουν να ενημερώσουν την Επιτροπή για τον ορισμό του ενιαίου κέντρου επαφής και τα καθήκοντά του μέχρι την εκπνοή της προθεσμίας μεταφοράς στο εθνικό δίκαιο. Ο ορισμός του ενιαίου κέντρου επαφής πρέπει να δημοσιοποιείται, κατά τον ίδιο τρόπο που δημοσιοποιούνται οι ορισθείσες εθνικές αρμόδιες αρχές. Η Επιτροπή δημοσιεύει τον κατάλογο των ενιαίων κέντρων επαφής που έχουν οριστεί.

3.7. Κυρώσεις

Το άρθρο 21 αφήνει περιθώριο στα κράτη μέλη να αποφασίζουν το είδος και τη φύση των κυρώσεων που θα επιβάλλουν, υπό την προϋπόθεση να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Με άλλα λόγια, τα κράτη μέλη είναι καταρχάς ελεύθερα να αποφασίζουν το μέγιστο ύψος των κυρώσεων που θα προβλέπονται στην εθνική τους νομοθεσία, όμως το ύψος ή ποσοστό των κυρώσεων που θα επιλεγεί θα πρέπει να επιτρέπει στις εθνικές αρχές να επιβάλλουν, σε κάθε συγκεκριμένη περίπτωση, αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις, λαμβάνοντας υπόψη διάφορους παράγοντες όπως η σοβαρότητα ή η συχνότητα της παράβασης.

4. Οντότητες που υπέχουν υποχρεώσεις δυνάμει των απαιτήσεων ασφάλειας και κοινοποίησης συμβάντων

Οι οντότητες που διαδραματίζουν σημαντικό ρόλο στην κοινωνία και την οικονομία, οι οποίες αναφέρονται στο άρθρο 4 παράγραφοι 4 και 6 της οδηγίας αντίστοιχα ως φορείς εκμετάλλευσης βασικών υπηρεσιών και πάροχοι ψηφιακών υπηρεσιών, οφείλουν να λαμβάνουν κατάλληλα μέτρα ασφαλείας και να κοινοποιούν τα σοβαρά συμβάντα στις αρμόδιες εθνικές αρχές. Η λογική στην οποία βασίζεται η συγκεκριμένη απαίτηση είναι ότι ο αντίκτυπος των συμβάντων ασφαλείας σε αυτές τις υπηρεσίες μπορεί να αποτελέσει μείζονα απειλή για τη λειτουργία των εν λόγω υπηρεσιών, καθώς είναι πιθανό να προκαλέσει σημαντικές διαταραχές στην άσκηση των οικονομικών δραστηριοτήτων και στην κοινωνία γενικότερα, υπονομεύοντας ενδεχομένως την εμπιστοσύνη των χρηστών και προκαλώντας σοβαρή ζημία στην οικονομία της Ένωσης[24].

Στην παρούσα ενότητα παρέχεται επισκόπηση των οντοτήτων που περιλαμβάνονται στο πεδίο εφαρμογής των παραρτημάτων ΙΙ και ΙΙΙ της οδηγίας ΑΔΠ και αναφέρονται αναλυτικά οι υποχρεώσεις τους. Καλύπτεται ακόμη εκτενώς ο προσδιορισμός των φορέων εκμετάλλευσης βασικών υπηρεσιών, δεδομένης της σημασίας της εν λόγω διαδικασίας για την εναρμονισμένη εφαρμογή της οδηγίας ΑΔΠ σε ολόκληρη την ΕΕ. Παρέχονται επίσης αναλυτικές διευκρινίσεις σχετικά με τους ορισμούς των ψηφιακών υποδομών και των παρόχων ψηφιακών υπηρεσιών. Επιπλέον, εξετάζεται η πιθανή συμπερίληψη πρόσθετων τομέων και επεξηγείται περαιτέρω η ειδική προσέγγιση σε σχέση με τους παρόχους ψηφιακών υπηρεσιών.

[24] Βλ. αιτιολογική σκέψη 2.

4.1. Φορείς εκμετάλλευσης βασικών υπηρεσιών

Η οδηγία ΑΔΠ δεν ορίζει ρητώς ποιες συγκεκριμένες οντότητες θα θεωρούνται ως φορείς εκμετάλλευσης βασικών υπηρεσιών που υπάγονται στο πεδίο εφαρμογής της. Αντ' αυτού, προβλέπει κριτήρια τα οποία θα πρέπει να λάβουν υπόψη τα κράτη μέλη κατά τη διεξαγωγή της διαδικασίας προσδιορισμού μέσω της οποίας θα καθοριστεί τελικώς ποιες μεμονωμένες εταιρείες οι οποίες ανήκουν στα είδη οντοτήτων που αναφέρονται στο παράρτημα ΙΙ θα θεωρηθούν ως φορείς εκμετάλλευσης βασικών υπηρεσιών και θα βαρύνονται επομένως με τις υποχρεώσεις που απορρέουν από την οδηγία.

4.1.1. Είδη οντοτήτων που αναφέρονται στο παράρτημα ΙΙ της οδηγίας ΑΔΠ

Σύμφωνα με τον ορισμό του άρθρου 4 σημείο 4, ως φορέας εκμετάλλευσης βασικών υπηρεσιών νοείται μια δημόσια ή ιδιωτική οντότητα είδους αναφερόμενου στο παράρτημα ΙΙ της οδηγίας η οποία πληροί τα κριτήρια που ορίζονται στο άρθρο 5 παράγραφος 2. Στο παράρτημα ΙΙ απαριθμούνται οι τομείς, οι υποτομείς και τα είδη οντοτήτων για τα οποία κάθε κράτος μέλος οφείλει να διεξαγάγει τη διαδικασία προσδιορισμού του άρθρου 5 παράγραφος 2[25]. Στους τομείς περιλαμβάνονται η ενέργεια, οι μεταφορές, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών, η υγεία, η ύδρευση και η ψηφιακή υποδομή.

Για την πλειονότητα των οντοτήτων που ανήκουν στην κατηγορία των «παραδοσιακών τομέων», η νομοθεσία της ΕΕ περιλαμβάνει επαρκώς ανεπτυγμένους ορισμούς στους οποίους παραπέμπει το παράρτημα ΙΙ. Δεν ισχύει το ίδιο, όμως, για τον τομέα της ψηφιακής υποδομής που αναφέρεται στο σημείο 7 του παραρτήματος ΙΙ, καθώς και για τα σημεία ανταλλαγής κίνησης διαδικτύου, τα συστήματα ονομάτων χώρου και τα μητρώα ονομάτων χώρου ανωτάτου επιπέδου. Έτσι, για την πλήρη αποσαφήνιση των εν λόγω ορισμών, παρατίθενται ακολούθως αναλυτικές διευκρινίσεις για καθέναν από αυτούς.

1) Σημείο ανταλλαγής κίνησης διαδικτύου (IXP)

Ο όρος «σημείο ανταλλαγής κίνησης διαδικτύου» (Internet Exchange Point - IXP) ορίζεται στο άρθρο 4 σημείο 13 και αποσαφηνίζεται περαιτέρω στην αιτιολογική σκέψη 18. Μπορεί να περιγραφεί ως δικτυακή υποδομή που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων και τεχνικά αυτόνομων συστημάτων, κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης διαδικτύου. Το σημείο ανταλλαγής κίνησης διαδικτύου μπορεί ακόμη να περιγραφεί ως μια φυσική τοποθεσία στην οποία τα διάφορα δίκτυα μπορούν να ανταλλάσσουν μεταξύ τους κίνηση διαδικτύου μέσω διακόπτη. Ο βασικός σκοπός των IXP είναι να επιτρέπουν την απευθείας διασύνδεση των δικτύων μέσω της ανταλλαγής και όχι μέσω ενός ή περισσότερων δικτύων τρίτων μερών. Ο πάροχος IXP δεν ευθύνεται κατά κανόνα για τη δρομολόγηση της κίνησης διαδικτύου, η οποία εμπίπτει στην αρμοδιότητα των παρόχων δικτύου. Τα πλεονεκτήματα της απευθείας διασύνδεσης είναι πολλά, όμως οι βασικοί λόγοι είναι το κόστος, ο χρόνος απόκρισης και το εύρος ζώνης. Στην κίνηση

[25] Βλ. ενότητα 4.1.6 ακολούθως για περισσότερες λεπτομέρειες σχετικά με τη διαδικασία προσδιορισμού

διαδικτύου που διέρχεται μέσω ανταλλαγής δεν επιβάλλεται κατά κανόνα καμία χρέωση, ενώ δεν συμβαίνει το ίδιο με την κυκλοφορία προς ανάντη φορέα παροχής υπηρεσιών στο διαδίκτυο (ISP). Με την απευθείας διασύνδεση, που βρίσκεται συνήθως στην ίδια πόλη με αμφότερα τα δίκτυα, αποφεύγεται η ανάγκη να διανύουν τα δεδομένα μεγάλες αποστάσεις για να φτάσουν από ένα δίκτυο σε άλλο, και μειώνεται έτσι ο χρόνος απόκρισης.

Θα πρέπει να σημειωθεί ότι ο ορισμός του IXP δεν καλύπτει τις φυσικές τοποθεσίες όπου διασυνδέονται μεταξύ τους μόνο δύο φυσικά δίκτυα (ήτοι, πάροχοι δικτύου όπως οι BASE και PROXIMUS). Επομένως, κατά τη μεταφορά της οδηγίας, τα κράτη μέλη πρέπει να κάνουν διάκριση ανάμεσα στους φορείς εκμετάλλευσης που διευκολύνουν την ανταλλαγή συγκεντρωτικής κίνησης διαδικτύου μεταξύ φορέων εκμετάλλευσης πολλών δικτύων και σε εκείνους που είναι φορείς εκμετάλλευσης ενός δικτύου, οι οποίοι διασυνδέουν με φυσικό τρόπο τα δίκτυά τους βάσει συμφωνίας διασύνδεσης. Οι πάροχοι δικτύου της δεύτερης περίπτωσης δεν καλύπτονται από τον ορισμό του άρθρου 4 σημείο 13. Το θέμα αυτό αποσαφηνίζεται περαιτέρω στην αιτιολογική σκέψη 18 όπου αναφέρεται ότι το IXP δεν παρέχει πρόσβαση στο δίκτυο ούτε ενεργεί ως πάροχος ή φορέας διαβατικών υπηρεσιών. Η τελευταία κατηγορία παρόχων είναι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό οι οποίες υπόκεινται στις υποχρεώσεις ασφάλειας και κοινοποίησης των άρθρων 13α και 13β της οδηγίας 2002/21/ΕΚ και επομένως αποκλείονται από το πεδίο εφαρμογής της οδηγίας ΑΔΠ[26].

2) Σύστημα ονομάτων χώρου (DNS)

Σύμφωνα με τον ορισμό του άρθρου 4 σημείο 14, ως «σύστημα ονομάτων χώρου» (Domain Name System - DNS) νοείται ένα *«ιεραρχικό κατανεμημένο σύστημα ονοματοδοσίας εντός ενός δικτύου το οποίο εκτελεί παραπομπές αιτημάτων για ονόματα τομέων»*. Πιο συγκεκριμένα, το DNS μπορεί να περιγραφεί ως ιεραρχικό κατανεμημένο σύστημα ονοματοδοσίας για υπολογιστές, υπηρεσίες ή άλλους πόρους συνδεδεμένους με το Διαδίκτυο που επιτρέπει την κωδικοποίηση ονομάτων χώρου σε διευθύνσεις IP (πρωτόκολλο Ίντερνετ). Ο βασικός ρόλος του συστήματος είναι να μεταφράζει τα εκχωρημένα ονόματα χώρου σε διευθύνσεις IP. Προς τούτο, το DNS διαθέτει βάση δεδομένων και χρησιμοποιεί διακομιστές ονομάτων και εφαρμογή επίλυσης ερωτημάτων (resolver) για να μπορέσει να κάνει αυτού του είδους τη «μετάφραση» των ονομάτων χώρου σε λειτουργικές διευθύνσεις IP. Η κωδικοποίηση ονομάτων χώρου δεν είναι μεν η μοναδική αρμοδιότητα του DNS, αποτελεί όμως πολύ βασικό καθήκον του συστήματος. Ο νομικός ορισμός του άρθρου 4 σημείο 14 εστιάζει στον κύριο ρόλο του συστήματος από τη σκοπιά των χρηστών χωρίς να υπεισέρχεται σε περισσότερο τεχνικές λεπτομέρειες, όπως για παράδειγμα τη λειτουργία του χώρου ονομάτων τομέα, των διακομιστών ονομάτων, των λυτών (resolvers) κ.λπ. Τέλος, στο άρθρο 4 σημείο 15 διευκρινίζεται ποιος θεωρείται πάροχος υπηρεσιών DNS.

3) Μητρώο ονομάτων χώρου ανωτάτου επιπέδου (μητρώο ονομάτων TLD)

[26] Βλ. ενότητα 5.2 για περισσότερες λεπτομέρειες όσον αφορά τη σχέση μεταξύ της οδηγίας ΑΔΠ και της οδηγίας 2002/21/ΕΚ.

Σύμφωνα με τον ορισμό του άρθρου 4 σημείο 16, ως «μητρώο ονομάτων χώρου ανωτάτου επιπέδου» νοείται μια οντότητα που διαχειρίζεται και εκμεταλλεύεται την καταχώριση ονομάτων διαδικτυακών χώρων εντός συγκεκριμένου χώρου ανωτάτου επιπέδου (TLD). Μέρος της εν λόγω εκμετάλλευσης και διαχείρισης ονομάτων χώρου είναι και η κωδικοποίηση των ονομάτων TLD σε διευθύνσεις IP.

Υπεύθυνη για τον συντονισμό σε παγκόσμιο επίπεδο του πυρήνα DNS (DNS Root), των διευθύνσεων πρωτοκόλλου Ίντερνετ (Internet Protocol - IP), καθώς και άλλων πόρων IP είναι η Αρχή του Διαδικτύου για την Εκχώρηση Αριθμών (Internet Assigned Numbers Authority - IANA). Συγκεκριμένα, η IANA είναι υπεύθυνη για την εκχώρηση χώρων ανωτάτου επιπέδου γενικού χαρακτήρα (gTLD), π.χ. «.com», και χώρων ανωτάτου επιπέδου ειδικά για κωδικούς χωρών (ccTLD), π.χ. «.be», σε φορείς εκμετάλλευσης (μητρώα), καθώς και για τη διατήρηση των αναλυτικών τους στοιχείων τεχνικής και διοικητικής φύσης. Η IANA διατηρεί μητρώο όλων των εκχωρημένων παγκοσμίως TLD και συμβάλλει στη διάδοση του εν λόγω καταλόγου στους χρήστες του Διαδικτύου ανά τον κόσμο, καθώς και στη δημιουργία νέων TLD.

Σημαντικό καθήκον των μητρώων είναι η εκχώρηση ονομάτων δεύτερου επιπέδου στους λεγόμενους καταχωρούμενους στον αντίστοιχο χώρο ανωτάτου επιπέδου (TLD). Οι εν λόγω καταχωρούμενοι έχουν επίσης τη δυνατότητα να επιλέξουν, εφόσον το επιθυμούν, να εκχωρούν οι ίδιοι ονόματα χώρων τρίτου επιπέδου. Οι χώροι ανωτάτου επιπέδου ειδικά για κωδικούς χωρών (ccTLD) φέρουν προσδιορισμό που αντιπροσωπεύει χώρες ή επικράτειες με βάση το πρότυπο ISO 3166-1, ενώ οι TLD «γενικού χαρακτήρα» δεν φέρουν κατά κανόνα προσδιορισμό συγκεκριμένης χώρας ή γεωγραφικής τοποθεσίας.

Θα πρέπει να σημειωθεί ότι η λειτουργία μητρώου ονομάτων TLD είναι δυνατόν να περιλαμβάνει και την παροχή DNS. Για παράδειγμα, σύμφωνα με τους κανόνες ανάθεσης αρμοδιοτήτων της IANA, η ορισθείσα οντότητα που ασχολείται με τους ccTLD πρέπει – μεταξύ άλλων – να έχει την εποπτεία των ονομάτων χώρου και τη λειτουργία του DNS της συγκεκριμένης χώρας[27]. Όλα αυτά πρέπει να ληφθούν υπόψη από τα κράτη μέλη κατά τη διεξαγωγή της διαδικασίας προσδιορισμού των φορέων εκμετάλλευσης βασικών υπηρεσιών δυνάμει του άρθρου 5 παράγραφος 2.

4.1.2. Προσδιορισμός φορέων εκμετάλλευσης βασικών υπηρεσιών

Σύμφωνα με τις απαιτήσεις του άρθρου 5 της οδηγίας, κάθε κράτος μέλος οφείλει να διεξαγάγει διαδικασία προσδιορισμού για όλες τις οντότητες των ειδών που αναφέρονται στο παράρτημα ΙΙ που είναι νομίμως εγκατεστημένες στην επικράτειά του. Ως αποτέλεσμα αυτής της διαδικασίας, όλες οι οντότητες που πληρούν τα κριτήρια του άρθρου 5 παράγραφος 2 θα προσδιοριστούν ως φορείς εκμετάλλευσης βασικών υπηρεσιών και θα υπόκεινται στις υποχρεώσεις ασφάλειας και κοινοποίησης του άρθρου 14.

Τα κράτη μέλη έχουν προθεσμία μέχρι τις 9 Νοεμβρίου 2018 για να προσδιορίσουν τους φορείς εκμετάλλευσης για κάθε τομέα και υποτομέα. Με γνώμονα την παροχή υποστήριξης

[27] Στοιχεία διαθέσιμα στη διεύθυνση: https://www.icann.org/resources/pages/delegation-2012-02-25-en

στα κράτη μέλη καθόλη την προαναφερθείσα διαδικασία, η ομάδα συνεργασίας καταρτίζει επί του παρόντος έγγραφο καθοδήγησης με πληροφορίες για τα απαιτούμενα βήματα και τις βέλτιστες πρακτικές σε σχέση με τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών.

Επιπλέον, σύμφωνα με το άρθρο 24 παράγραφος 2, η ομάδα συνεργασίας θα συζητά τη διαδικασία, την ουσία και τον τύπο των εθνικών μέτρων για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών σε συγκεκριμένους τομείς. Ένα κράτος μέλος μπορεί επίσης, κατόπιν αιτήματός του, να συζητήσει με την ομάδα συνεργασίας, πριν από τις 9 Νοεμβρίου 2018, τα σχέδια εθνικών μέτρων που έχει καταρτίσει για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών.

4.1.3. Συμπερίληψη πρόσθετων τομέων

Λαμβάνοντας υπόψη την απαίτηση της ελάχιστης εναρμόνισης του άρθρου 3, τα κράτη μέλη μπορούν να θεσπίζουν ή να διατηρούν νομοθετικές διατάξεις που διασφαλίζουν υψηλότερο επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών. Ως προς το συγκεκριμένο θέμα, τα κράτη μέλη είναι γενικώς ελεύθερα να επεκτείνουν τις υποχρεώσεις ασφάλειας και κοινοποίησης του άρθρου 14 σε οντότητες άλλων τομέων και υποτομέων πέραν των αναφερόμενων στο παράρτημα ΙΙ της οδηγίας ΑΔΠ. Κάποια κράτη μέλη έχουν αποφασίσει ή εξετάζουν επί του παρόντος το ενδεχόμενο να συμπεριλάβουν ορισμένους από τους ακόλουθους πρόσθετους τομείς:

i) Φορείς δημόσιας διοίκησης

Οι φορείς δημόσιας διοίκησης μπορούν να παρέχουν βασικές υπηρεσίες του παραρτήματος ΙΙ της οδηγίας που συμμορφώνονται με τις απαιτήσεις του άρθρου 5 παράγραφος 2. Σε αυτές τις περιπτώσεις, οι φορείς δημόσιας διοίκησης που παρέχουν βασικές υπηρεσίες θα διέπονται από τις συναφείς απαιτήσεις ασφαλείας και υποχρεώσεις κοινοποίησης. Αντίθετα, όταν οι φορείς δημόσιας διοίκησης παρέχουν υπηρεσίες που δεν εμπίπτουν στο πεδίο εφαρμογής του παραρτήματος ΙΙ, οι υπηρεσίες τους δεν θα διέπονται από τις συναφείς υποχρεώσεις.

Οι φορείς δημόσιας διοίκησης είναι υπεύθυνοι για την ορθή παροχή δημόσιων υπηρεσιών από κρατικές υπηρεσίες, περιφερειακές και τοπικές αρχές, οργανισμούς και συνδεδεμένες επιχειρήσεις. Η παροχή των εν λόγω υπηρεσιών προϋποθέτει συχνά τη δημιουργία και διαχείριση προσωπικών και εταιρικών δεδομένων για άτομα και οργανισμούς, τα οποία μπορούν να αποτελέσουν αντικείμενο ανταλλαγής και να διατεθούν σε διάφορες δημόσιες οντότητες. Γενικότερα, το υψηλό επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι φορείς δημόσιας διοίκησης αποτελεί σημαντικό όφελος για την κοινωνία και την οικονομία συνολικά. Η Επιτροπή εκτιμά επομένως ότι θα ήταν συνετό να εξετάσουν τα κράτη μέλη το ενδεχόμενο συμπερίληψης των φορέων δημόσιας διοίκησης στο πεδίο εφαρμογής της νομοθεσίας με την οποία θα μεταφερθεί στα εθνικά δίκαια η οδηγία, πέραν της παροχής βασικών υπηρεσιών κατά τα προβλεπόμενα στο παράρτημα ΙΙ και στο άρθρο 5 παράγραφος 2.

ii) Ταχυδρομικός τομέας

Ο ταχυδρομικός τομέας περιλαμβάνει την παροχή ταχυδρομικών υπηρεσιών όπως η συλλογή, διαλογή, μεταφορά και διανομή ταχυδρομικών αντικειμένων.

iii) Τομέας των τροφίμων

Ο τομέας των τροφίμων αφορά την παραγωγή γεωργικών προϊόντων και άλλων ειδών διατροφής και μπορεί να περιλαμβάνει την παροχή βασικών υπηρεσιών όπως η επισιτιστική ασφάλεια και η διασφάλιση της ποιότητας και της ασφάλειας των τροφίμων.

iv) Χημική και πυρηνική βιομηχανία

Η χημική και πυρηνική βιομηχανία αφορά συγκεκριμένα την αποθήκευση, παραγωγή και επεξεργασία χημικών και πετροχημικών προϊόντων ή πυρηνικών υλικών.

v) Περιβαλλοντικός τομέας

Στις περιβαλλοντικές δραστηριότητες περιλαμβάνεται η παροχή προϊόντων και υπηρεσιών που είναι αναγκαία για την προστασία του περιβάλλοντος και τη διαχείριση των πόρων. Σκοπός, επομένως, των εν λόγω δραστηριοτήτων είναι η πρόληψη, η μείωση και η εξάλειψη της ρύπανσης, καθώς και η διατήρηση των αποθεμάτων των διαθέσιμων φυσικών πόρων. Βασικές υπηρεσίες που παρέχονται στο πλαίσιο του συγκεκριμένου τομέα θα μπορούσαν να είναι η παρακολούθηση και ο έλεγχος της ρύπανσης (π.χ. του αέρα και των υδάτων) και των μετεωρολογικών φαινομένων.

vi) Πολιτική προστασία

Στόχος του τομέα της πολιτικής προστασίας είναι η πρόληψη, η προετοιμασία για την αντιμετώπιση και η αντιμετώπιση φυσικών και ανθρωπογενών καταστροφών. Υπηρεσίες που παρέχονται για τον συγκεκριμένο σκοπό μπορεί να είναι η ενεργοποίηση αριθμών έκτακτης ανάγκης και η υλοποίηση δράσεων ενημέρωσης, περιορισμού και αντιμετώπισης καταστάσεων έκτακτης ανάγκης.

4.1.4. Δικαιοδοσία

Σύμφωνα με το άρθρο 5 παράγραφος 1, κάθε κράτος μέλος οφείλει να προσδιορίσει τους φορείς εκμετάλλευσης βασικών υπηρεσιών που είναι εγκατεστημένοι στην επικράτειά του. Η συγκεκριμένη διάταξη δεν προσδιορίζει περαιτέρω το είδος της νόμιμης εγκατάστασης, όμως στην αιτιολογική σκέψη 21 διευκρινίζεται ότι η εγκατάσταση προϋποθέτει την ουσιαστική και πραγματική άσκηση δραστηριότητας μέσω σταθερών σχημάτων, ενώ η νομική μορφή των σχημάτων αυτών δεν θα πρέπει να αποτελεί καθοριστικό παράγοντα. Αυτό σημαίνει ότι ένα κράτος μέλος μπορεί να έχει δικαιοδοσία πάνω σε έναν φορέα εκμετάλλευσης βασικών υπηρεσιών όχι μόνο όταν ο τελευταίος έχει την έδρα του στην επικράτεια του εν λόγω κράτους μέλους, αλλά και όταν διατηρεί σε αυτήν παράρτημα ή άλλου είδους νόμιμη εγκατάσταση.

Αυτό έχει ως συνέπεια ότι επί της ίδιας οντότητας μπορούν να έχουν ταυτόχρονα δικαιοδοσία περισσότερα από ένα κράτη μέλη.

4.1.5. Πληροφορίες που υποβάλλονται στην Επιτροπή

Για τους σκοπούς της επανεξέτασης που πρέπει να εκπονήσει η Επιτροπή δυνάμει του άρθρου 23 παράγραφος 1 της οδηγίας ΑΔΠ, τα κράτη μέλη οφείλουν να υποβάλουν στην Επιτροπή, έως τις 9 Νοεμβρίου 2018, και ανά διετία στη συνέχεια, τις ακόλουθες πληροφορίες:

- τα εθνικά μέτρα που επιτρέπουν τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών·

- τον κατάλογο βασικών υπηρεσιών·

- τον αριθμό των φορέων εκμετάλλευσης βασικών υπηρεσιών που έχουν προσδιοριστεί για κάθε τομέα που περιλαμβάνεται στο παράρτημα ΙΙ και τη σημασία τους για τον τομέα· και

- εφόσον υπάρχουν, τα κατώτατα όρια που χρησιμοποιούνται για τον προσδιορισμό του σχετικού επιπέδου παροχής με αναφορά στον αριθμό των χρηστών που εξαρτώνται από την υπηρεσία αυτή όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στη σημασία της οντότητας σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ).

Η επανεξέταση που προβλέπεται στο άρθρο 23 παράγραφος 1, η οποία προηγείται της συνολικής επανεξέτασης της οδηγίας, αντικατοπτρίζει τη σημασία που αποδίδουν οι συννομοθέτες στην ορθή μεταφορά της οδηγίας ως προς το σκέλος του προσδιορισμού των φορέων εκμετάλλευσης βασικών υπηρεσιών ώστε να αποφευχθεί ο κατακερματισμός της αγοράς.

Για τη διεξαγωγή της εν λόγω διαδικασίας κατά τον καλύτερο δυνατό τρόπο, η Επιτροπή ενθαρρύνει τα κράτη μέλη να συζητήσουν το συγκεκριμένο θέμα και να ανταλλάξουν σχετικές εμπειρίες στους κόλπους της ομάδας συνεργασίας. Η Επιτροπή ενθαρρύνει επιπλέον τα κράτη μέλη να της υποβάλουν - εμπιστευτικά, εφόσον απαιτείται - τους καταλόγους των προσδιορισμένων φορέων εκμετάλλευσης βασικών υπηρεσιών (που επιλέχθηκαν τελικά), επιπροσθέτως όλων των άλλων πληροφοριών που οφείλουν να της υποβάλουν δυνάμει της οδηγίας. Εάν οι σχετικοί κατάλογοι τεθούν στη διάθεση της Επιτροπής, θα της επιτρέψουν να αξιολογήσει ευκολότερα και καλύτερα τη συνοχή της διαδικασίας προσδιορισμού, και επιπλέον θα επιτρέψουν τη σύγκριση μεταξύ των προσεγγίσεων που ακολουθούν τα διάφορα κράτη μέλη, συμβάλλοντας έτσι στην καλύτερη επίτευξη των στόχων της οδηγίας.

4.1.6. Τρόπος διεξαγωγής της διαδικασίας προσδιορισμού

Όπως απεικονίζεται στο σχήμα 4, υπάρχουν έξι βασικά ερωτήματα στα οποία θα πρέπει να απαντήσει η εκάστοτε εθνική αρχή στο πλαίσιο της διαδικασίας προσδιορισμού κάθε επιμέρους οντότητας. Ακολούθως παρατίθενται πέντε ερωτήματα που αντιστοιχούν στα βήματα που πρέπει να γίνουν σύμφωνα με το άρθρο 5 σε συνδυασμό με το άρθρο 6, λαμβανομένης επιπλέον υπόψη της εφαρμογής ή όχι του άρθρου 1 παράγραφος 7.

Βήμα 1 – **Η οντότητα ανήκει σε τομέα/υποτομέα & αντιστοιχεί σε είδος του παραρτήματος ΙΙ της οδηγίας;**

Η εθνική αρχή θα πρέπει να προσδιορίσει εάν μια οντότητα εγκατεστημένη στην επικράτειά της ανήκει σε κάποιον από τους τομείς και υποτομείς που αναφέρονται στο παράρτημα ΙΙ της οδηγίας. Το παράρτημα ΙΙ καλύπτει διάφορους οικονομικούς τομείς που θεωρούνται καίριας

σημασίας για τη διασφάλιση της ορθής λειτουργίας της εσωτερικής αγοράς. Συγκεκριμένα, στο παράρτημα ΙΙ αναφέρονται οι ακόλουθοι τομείς και υποτομείς:

- Ενέργεια: ηλεκτρική ενέργεια, πετρέλαιο και αέριο
- Μεταφορές: αεροπορικές, σιδηροδρομικές, πλωτές και οδικές
- Τράπεζες: πιστωτικά ιδρύματα
- Υποδομές χρηματοπιστωτικών αγορών: τόποι διαπραγμάτευσης, κεντρικοί αντισυμβαλλόμενοι
- Υγεία: πάροχοι υγειονομικής περίθαλψης (μεταξύ άλλων νοσοκομεία και ιδιωτικές κλινικές)
- Νερό: προμήθεια και διανομή πόσιμου νερού
- Ψηφιακή υποδομή: σημεία ανταλλαγής κίνησης διαδικτύου, πάροχοι υπηρεσιών συστήματος ονομάτων χώρου, μητρώα ονομάτων χώρου ανώτατου επιπέδου[28]

Βήμα 2 – **Εφαρμόζεται η διάταξη περί *lex specialis*;**

Το επόμενο βήμα είναι να προσδιορίσει η εθνική αρχή εάν εφαρμόζεται η διάταξη περί *lex specialis* του άρθρου 1 παράγραφος 7. Συγκεκριμένα, η διάταξη ορίζει ότι εάν υφίσταται νομική πράξη της ΕΕ που επιβάλλει απαιτήσεις ασφάλειας και/ή κοινοποίησης στους παρόχους ψηφιακών υπηρεσιών ή στους φορείς εκμετάλλευσης βασικών υπηρεσιών οι οποίες είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που θεσπίζονται στην οδηγία ΑΔΠ, θα εφαρμόζονται οι διατάξεις της ειδικής νομικής πράξης. Στην αιτιολογική σκέψη 9 διευκρινίζεται περαιτέρω ότι αν πληρούνται οι απαιτήσεις του άρθρου 1 παράγραφος 7, τα κράτη μέλη θα πρέπει να εφαρμόζουν τις διατάξεις της τομεακής πράξης της Ένωσης, συμπεριλαμβανομένων εκείνων που αφορούν τη δικαιοδοσία, και όχι τις συναφείς διατάξεις της οδηγίας ΑΔΠ. Στην προκειμένη περίπτωση, η αρμόδια αρχή δεν θα πρέπει να συνεχίζει τη διαδικασία προσδιορισμού του άρθρου 5 παράγραφος 2[29].

Βήμα 3 – **Ο φορέας εκμετάλλευσης παρέχει ουσιώδη υπηρεσία που εμπίπτει στην έννοια της οδηγίας;**

Σύμφωνα με το άρθρο 5 παράγραφος 2 στοιχείο α), η οντότητα για την οποία διεξάγεται η διαδικασία προσδιορισμού πρέπει να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών και/ή οικονομικών δραστηριοτήτων. Κατά τη διεξαγωγή της διαδικασίας προσδιορισμού, τα κράτη μέλη θα πρέπει να λαμβάνουν υπόψη ότι μία οντότητα είναι δυνατό να παρέχει ταυτόχρονα ουσιώδεις και μη ουσιώδεις υπηρεσίες. Αυτό σημαίνει ότι οι απαιτήσεις ασφάλειας και κοινοποίησης της οδηγίας ΑΔΠ θα βαρύνουν τον εκάστοτε φορέα εκμετάλλευσης μόνο ως προς τις ουσιώδεις υπηρεσίες που παρέχει.

Σύμφωνα με το άρθρο 5 παράγραφος 3, κάθε κράτος μέλος θα πρέπει να καταρτίσει κατάλογο όλων των ουσιωδών υπηρεσιών που παρέχονται από φορείς εκμετάλλευσης

[28]Αναλυτικότερες πληροφορίες για τις προαναφερθείσες οντότητες παρατίθενται στην ενότητα 4.1.1.

[29] Περισσότερες πληροφορίες για την εφαρμογή της διάταξης περί *lex specialis* παρέχονται στην ενότητα 5.1.

βασικών υπηρεσιών στην επικράτειά του. Ο εν λόγω κατάλογος θα πρέπει να υποβληθεί στην Επιτροπή έως τις 9 Νοεμβρίου 2018, και ανά διετία στη συνέχεια[30].

Βήμα 4 - **Η υπηρεσία στηρίζεται σε σύστημα δικτύου και πληροφοριών;**

Στη συνέχεια θα πρέπει να διευκρινιστεί αν η συγκεκριμένη υπηρεσία πληροί το δεύτερο κριτήριο του άρθρου 5 παράγραφος 2 στοιχείο β) και συγκεκριμένα αν η παροχή της βασικής υπηρεσίας στηρίζεται σε συστήματα δικτύου και πληροφοριών κατά τα οριζόμενα στο άρθρο 4 παράγραφος 1.

Βήμα 5 – **Τυχόν συμβάν ασφαλείας θα προκαλούσε σοβαρή διατάραξη;**

Σύμφωνα με το άρθρο 5 παράγραφος 2 στοιχείο γ), η εθνική αρχή οφείλει να προσδιορίσει εάν τυχόν συμβάν θα προκαλούσε σοβαρή διατάραξη της παροχής της εν λόγω υπηρεσίας. Στο πλαίσιο αυτό, το άρθρο 6 παράγραφος 1 προβλέπει διάφορους διατομεακούς παράγοντες που πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό της σοβαρότητας διατάραξης. Το άρθρο 6 παράγραφος 2 προβλέπει περαιτέρω ότι θα πρέπει να λαμβάνονται επίσης υπόψη, ανάλογα με την περίπτωση, παράγοντες που αφορούν συγκεκριμένους τομείς.

Οι **διατομεακοί παράγοντες** που αναφέρονται στο άρθρο 6 παράγραφος 1 είναι οι ακόλουθοι:

- ο αριθμός των χρηστών που εξαρτώνται από την υπηρεσία που παρέχεται από την οικεία οντότητα·
- η εξάρτηση άλλων τομέων που αναφέρονται στο παράρτημα ΙΙ από την υπηρεσία που παρέχεται από την εν λόγω οντότητα·
- ο αντίκτυπος που θα μπορούσαν να έχουν τα συμβάντα, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια·
- το μερίδιο αγοράς της εν λόγω οντότητας·
- το γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα συμβάν·
- η σημασία του φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας.

Όσον αφορά τους **παράγοντες που αφορούν συγκεκριμένους τομείς**, στην αιτιολογική σκέψη 28 παρατίθενται ορισμένα παραδείγματα (βλ. πίνακα 4) τα οποία θα μπορούσαν να χρησιμεύσουν ως καθοδήγηση για τις εθνικές αρχές.

Πίνακας 4: Παραδείγματα ειδικών ανά τομέα παραγόντων που πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό της σοβαρότητας διατάραξης σε περίπτωση συμβάντος.

[30] Βλέπε άρθρο 5 παράγραφος 7 στοιχείο β)

Τομέας	Παραδείγματα ειδικών ανά τομέα παραγόντων
Προμηθευτές ενέργειας	όγκος ή μερίδιο επί της παραγόμενης ενέργειας σε εθνικό επίπεδο
Προμηθευτές πετρελαίου	ημερήσιος όγκος παρεχόμενου πετρελαίου
Αεροπορικές μεταφορές (συμπεριλαμβανομένων των αερολιμένων και των αερομεταφορέων) **Σιδηροδρομικές μεταφορές** **Θαλάσσιοι λιμένες**	μερίδιο επί του όγκου διακίνησης επιβατών σε εθνικό επίπεδο· αριθμός επιβατών ή μεταφορών φορτίου ανά έτος.
Τράπεζες ή υποδομές χρηματοπιστωτικής αγοράς	συστημική σημασία με βάση το συνολικό ενεργητικό· λόγος συνολικού ενεργητικού προς ΑΕΠ
Τομέας της υγείας	αριθμός ασθενών που λαμβάνουν τις υπηρεσίες υγείας του παρόχου ανά έτος
Παραγωγή, επεξεργασία και παροχή νερού	όγκος και αριθμός καθώς και είδη χρηστών (συμπεριλαμβανομένων, για παράδειγμα, νοσοκομείων, δημόσιων υπηρεσιών, οργανισμών, ή ιδιωτών)· ύπαρξη εναλλακτικών πηγών νερού που καλύπτουν την ίδια γεωγραφική περιοχή

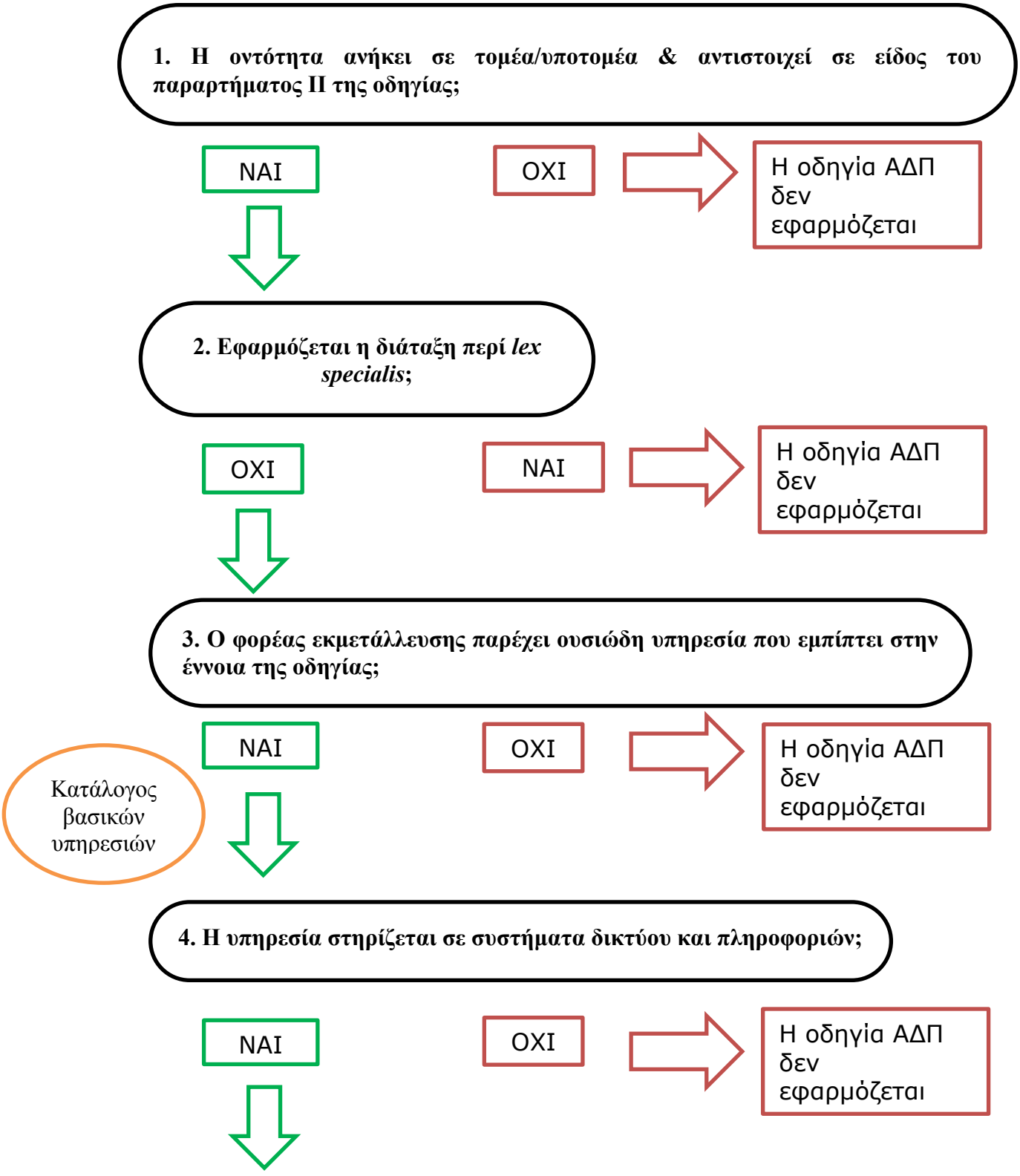
Θα πρέπει να επισημανθεί ότι στο πλαίσιο της διαδικασίας προσδιορισμού του άρθρου 5 παράγραφος 2, τα κράτη μέλη δεν θα πρέπει να προβλέπουν πρόσθετα κριτήρια πέραν εκείνων που αναφέρονται στη συγκεκριμένη διάταξη, καθώς αυτό θα μπορούσε να οδηγήσει σε περιορισμό του αριθμού των προσδιορισμένων φορέων εκμετάλλευσης βασικών υπηρεσιών και να υπονομεύσει την ελάχιστη εναρμόνιση που προβλέπεται στο άρθρο 3 της οδηγίας για τους φορείς εκμετάλλευσης βασικών υπηρεσιών.

Βήμα 6 - **Ο υπό εξέταση φορέας εκμετάλλευσης παρέχει βασικές υπηρεσίες σε άλλα κράτη μέλη;**

Το βήμα 6 αφορά περιπτώσεις στις οποίες ο φορέας εκμετάλλευσης παρέχει τις βασικές υπηρεσίες του σε δύο ή περισσότερα κράτη μέλη. Σύμφωνα με το άρθρο 5 παράγραφος 4, τα εμπλεκόμενα κράτη μέλη οφείλουν να προβαίνουν σε διαβούλευση μεταξύ τους πριν από τη λήψη απόφασης για τον προσδιορισμό[31].

[31] Για περισσότερες πληροφορίες σχετικά με τη διαδικασία διαβούλευσης, βλ. ενότητα 4.1.7.

Σχήμα 4: Διαδικασία προσδιορισμού σε 6 βήματα.



5. Τυχόν συμβάν ασφαλείας θα προκαλούσε σοβαρή διατάραξη;

Διατομεακοί παράγοντες (άρθρο 6 παράγραφος 1)

- **Αριθμός χρηστών** που εξαρτώνται από τις υπηρεσίες
- **Εξάρτηση** άλλων βασικών τομέων από την υπηρεσία
- Αντίκτυπος που θα μπορούσαν να έχουν τα συμβάντα σε **οικονομικές και κοινωνικές δραστηριότητες** ή **στη δημόσια ασφάλεια**
- Πιθανό **γεωγραφικό εύρος**

ας

Παράγοντες που αφορούν συγκεκριμένους τομείς (παραδείγματα που αναφέρονται στην αιτιολογική σκέψη 28)

- **Ενέργεια**: όγκος ή μερίδιο επί της παραγόμενης ενέργειας σε εθνικό επίπεδο
- **Μεταφορές**: μερίδιο επί του όγκου διακίνησης επιβατών σε εθνικό επίπεδο & αριθμός μεταφορών ανά έτος

ΝΑΙ

ΟΧΙ → Η οδηγία ΑΔΠ δεν εφαρμόζεται

6. Ο υπό εξέταση φορέας εκμετάλλευσης παρέχει βασικές υπηρεσίες σε άλλα κράτη μέλη;

ΝΑΙ

ΟΧΙ → Η οδηγία ΑΔΠ δεν εφαρμόζεται

Υποχρεωτική διαβούλευση με το ή τα εμπλεκόμενα ΚΜ

Έγκριση εθνικών μέτρων (π.χ. κατάλογο φορέων εκμετάλλευσης βασικών υπηρεσιών, πολιτικά και νομικά μέτρα).

4.1.7. Διασυνοριακή διαδικασία διαβούλευσης

Όταν ένας φορέας εκμετάλλευσης παρέχει βασικές υπηρεσίες σε δύο ή περισσότερα κράτη μέλη, το άρθρο 5 παράγραφος 4 προβλέπει ότι τα εν λόγω κράτη μέλη προβαίνουν σε διαβούλευση μεταξύ τους πριν από τη λήψη απόφασης για τον προσδιορισμό. Σκοπός της εν λόγω διαβούλευσης είναι να διευκολυνθεί η αξιολόγηση της κρίσιμης φύσης του φορέα εκμετάλλευσης ως προς τον διασυνοριακό αντίκτυπο.

Το επιθυμητό αποτέλεσμα της διαβούλευσης είναι να ανταλλάξουν μεταξύ τους οι εμπλεκόμενες εθνικές αρχές επιχειρήματα και θέσεις και ιδανικά να καταλήξουν στην ίδια απόφαση σχετικά με τον προσδιορισμό του υπό εξέταση φορέα εκμετάλλευσης. Η οδηγία ΑΔΠ δεν αποκλείει, πάντως, να καταλήξουν τα κράτη μέλη σε διαφορετικά συμπεράσματα όσον αφορά τον προσδιορισμό ή όχι μιας συγκεκριμένης οντότητας ως φορέα εκμετάλλευσης βασικών υπηρεσιών. Στην αιτιολογική σκέψη 24 αναφέρεται ότι τα κράτη μέλη έχουν τη δυνατότητα να ζητήσουν τη συνδρομή της ομάδας συνεργασίας στο συγκεκριμένο θέμα.

Η Επιτροπή φρονεί ότι τα κράτη μέλη θα πρέπει να επιδιώκουν την επίτευξη συναίνεσης στο συγκεκριμένο θέμα ώστε να αποφεύγεται το ενδεχόμενο η ίδια εταιρεία να έχει διαφορετικό νομικό καθεστώς στα διάφορα κράτη μέλη. Απόκλιση θα πρέπει να υπάρχει σε εξαιρετικές περιπτώσεις, π.χ., όταν μια οντότητα προσδιορισμένη ως φορέας εκμετάλλευσης βασικών υπηρεσιών σε ένα κράτος μέλος έχει ελάχιστη και αμελητέα δραστηριότητα σε κάποιο άλλο.

4.2. Απαιτήσεις ασφάλειας

Σύμφωνα με το άρθρο 14 παράγραφος 1, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών, έχοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι οργανισμοί κατά την παροχή των υπηρεσιών τους. Σύμφωνα με το άρθρο 14 παράγραφος 2, τα κατάλληλα μέτρα λαμβάνονται με γνώμονα την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων.

Στους κόλπους της ομάδας συνεργασίας έχει συσταθεί ειδική ομάδα εργασίας η οποία ασχολείται επί του παρόντος με την κατάρτιση μη δεσμευτικών κατευθυντήριων γραμμών σχετικά με τα μέτρα ασφαλείας για φορείς εκμετάλλευσης βασικών υπηρεσιών[32]. Η σύνταξη του εγγράφου καθοδήγησης αναμένεται να έχει ολοκληρωθεί από την ομάδα ως το τέταρτο τρίμηνο του 2017. Η Επιτροπή ενθαρρύνει τα κράτη μέλη να εφαρμόσουν κατά γράμμα το έγγραφο καθοδήγησης που καταρτίζεται επί του παρόντος από την ομάδα συνεργασίας, ώστε να επιτευχθεί η μέγιστη δυνατή ευθυγράμμιση των εθνικών διατάξεων για τις απαιτήσεις ασφάλειας. Η εναρμόνιση των εν λόγω απαιτήσεων αναμένεται να διευκολύνει σημαντικά τη

[32] Για τους σκοπούς της προαναφερθείσας ομάδας εργασίας, καταρτίστηκαν και χρησιμοποιήθηκαν ως συνεισφορές για τους τομείς και τα μέτρα ασφάλειας που προτείνονται κατάλογοι με διεθνή πρότυπα, ορθές πρακτικές και μεθοδολογίες εκτίμησης/διαχείρισης για όλους τους τομείς που καλύπτονται από την οδηγία ΑΔΠ.

συμμόρφωση των φορέων εκμετάλλευσης βασικών υπηρεσιών οι οποίοι παρέχουν συνήθως βασικές υπηρεσίες σε περισσότερα από ένα κράτη μέλη, καθώς και τα καθήκοντα εποπτείας των εθνικών αρμόδιων αρχών και των CSIRT.

4.3 Απαιτήσεις κοινοποίησης

Σύμφωνα με το άρθρο 14 παράγραφος 3, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών κοινοποιούν «*συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών*». Συνεπώς, οι φορείς εκμετάλλευσης βασικών υπηρεσιών δεν θα πρέπει να κοινοποιούν ήσσονος σημασίας συμβάντα αλλά μόνο σοβαρά συμβάντα που επηρεάζουν τη συνέχεια της βασικής υπηρεσίας. Σύμφωνα με τον ορισμό του άρθρου 4 σημείο 7, ως συμβάν νοείται «*κάθε γεγονός που έχει στη πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών*». Επίσης, σύμφωνα με τον ορισμό του άρθρου 4 σημείο 2, ως «ασφάλεια συστημάτων δικτύου και πληροφοριών» νοείται «*η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών*». Συνεπώς, η υποχρέωση κοινοποίησης μπορεί να ενεργοποιηθεί δυνητικά από οποιοδήποτε συμβάν έχει δυσμενή επίπτωση όχι μόνο στη διαθεσιμότητα αλλά και στην αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων ή των συναφών υπηρεσιών. Πράγματι, η συνέχεια της υπηρεσίας που αναφέρεται στο άρθρο 14 παράγραφος 3 μπορεί να υπονομευθεί όχι μόνο σε περιπτώσεις που σχετίζονται με τη φυσική διαθεσιμότητα, αλλά και από κάθε άλλο συμβάν ασφαλείας που επηρεάζει την ορθή παροχή της υπηρεσίας[33].

Στους κόλπους της ομάδας συνεργασίας έχει συσταθεί ειδική ομάδα εργασίας η οποία καταρτίζει επί του παρόντος μη δεσμευτικές κατευθυντήριες γραμμές για την κοινοποίηση συμβάντων. Οι εν λόγω κατευθυντήριες γραμμές αφορούν συγκεκριμένα τις περιστάσεις στις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών οφείλουν να κοινοποιούν συμβάντα δυνάμει του άρθρου 14 παράγραφος 7, καθώς και τη μορφή και τη διαδικασία των εθνικών κοινοποιήσεων. Η σύνταξη των κατευθυντήριων γραμμών αναμένεται να έχει ολοκληρωθεί έως το τέταρτο τρίμηνο του 2017.

Η ύπαρξη διαφορετικών εθνικών απαιτήσεων κοινοποίησης ενδέχεται να οδηγήσει σε νομική αβεβαιότητα, συνθετότερες και επαχθέστερες διαδικασίες, καθώς και να συνεπάγεται σημαντικό διοικητικό κόστος για παρόχους που λειτουργούν διασυνοριακά. Η Επιτροπή εκφράζει επομένως την ικανοποίησή της για τις εργασίες της ομάδας συνεργασίας. Όπως και για τις απαιτήσεις ασφαλείας, η Επιτροπή ενθαρρύνει τα κράτη μέλη να εφαρμόσουν κατά γράμμα το έγγραφο καθοδήγησης που καταρτίζεται επί του παρόντος από την ομάδα συνεργασίας, ώστε να επιτευχθεί η μέγιστη δυνατή ευθυγράμμιση των εθνικών διατάξεων για τις κοινοποιήσεις συμβάντων.

[33] Το ίδιο ισχύει και για τους παρόχους ψηφιακών υπηρεσιών.

4.4. Οδηγία ΑΔΠ, παράρτημα ΙΙΙ: Πάροχοι ψηφιακών υπηρεσιών

Οι πάροχοι ψηφιακών υπηρεσιών είναι η δεύτερη κατηγορία οντοτήτων που περιλαμβάνεται στο πεδίο εφαρμογής της οδηγίας ΑΔΠ. Οι εν λόγω οντότητες θεωρούνται σημαντικοί οικονομικοί παράγοντες διότι χρησιμοποιούνται από πολλές επιχειρήσεις για την παροχή των δικών τους υπηρεσιών, και διότι τυχόν διατάραξη της ψηφιακής υπηρεσίας θα μπορούσε να έχει επιπτώσεις στις βασικές οικονομικές και κοινωνικές δραστηριότητες.

4.4.1. Κατηγορίες παρόχων ψηφιακών υπηρεσιών

Το άρθρο 4 σημείο 5 όπου ορίζεται η ψηφιακή υπηρεσία παραπέμπει στον νομικό ορισμό του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535 περιορίζοντας το πεδίο εφαρμογής στα είδη υπηρεσιών που αναφέρονται στο παράρτημα ΙΙΙ της οδηγίας ΑΔΠ. Έτσι, σύμφωνα με τον ορισμό του άρθρου 1 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2015/1535, ως ψηφιακή υπηρεσία νοείται «*κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν συγκεκριμένης παραγγελίας ενός αποδέκτη υπηρεσιών*», ενώ στο παράρτημα ΙΙΙ της οδηγίας ΑΔΠ παρατίθενται συγκεκριμένα τρία είδη ψηφιακών υπηρεσιών: επιγραμμική αγορά, επιγραμμική μηχανή αναζήτησης και υπηρεσία νεφοϋπολογιστικής. Σε αντίθεση με ό,τι προβλέπει για τους φορείς εκμετάλλευσης βασικών υπηρεσιών, η οδηγία δεν απαιτεί από τα κράτη μέλη να προβούν σε προσδιορισμό των παρόχων ψηφιακών υπηρεσιών, οι οποίοι θα όφειλαν ακολούθως να τηρούν τις σχετικές υποχρεώσεις. Συνεπώς, οι σχετικές υποχρεώσεις της οδηγίας, συγκεκριμένα δε οι απαιτήσεις για την ασφάλεια και τις κοινοποιήσεις που προβλέπονται στο άρθρο 16, θα ισχύουν για όλους τους παρόχους ψηφιακών υπηρεσιών που εμπίπτουν στο πεδίο εφαρμογής της.

Στις ακόλουθες ενότητες παρέχονται πρόσθετες διευκρινίσεις για τα τρία είδη ψηφιακών υπηρεσιών που περιλαμβάνονται στο πεδίο εφαρμογής της οδηγίας.

1. Πάροχος υπηρεσιών επιγραμμικής αγοράς

Η επιγραμμική αγορά επιτρέπει σε πολυάριθμες επιχειρήσεις ποικίλων κλάδων να ασκούν τις εμπορικές τους δραστηριότητες έναντι των καταναλωτών και να αναπτύσσουν σχέσεις με άλλες επιχειρήσεις. Παρέχει στις εταιρείες τη βασική υποδομή για επιγραμμικές και διασυνοριακές εμπορικές συναλλαγές. Οι πάροχοι υπηρεσιών επιγραμμικής αγοράς διαδραματίζουν σημαντικό ρόλο στην οικονομία ιδίως διότι παρέχουν πρόσβαση στις ΜΜΕ στην ευρύτερη ψηφιακή ενιαία αγορά της ΕΕ. Στις δραστηριότητες ενός παρόχου υπηρεσιών επιγραμμικής αγοράς είναι δυνατό να περιλαμβάνονται ακόμη η παροχή εξ αποστάσεως υπηρεσιών υπολογιστικής που διευκολύνουν την οικονομική δραστηριότητα των πελατών του, συμπεριλαμβανομένης της επεξεργασίας συναλλαγών και της συγκέντρωσης δεδομένων για τους αγοραστές, τους προμηθευτές και τα προϊόντα, καθώς και η διευκόλυνση της αναζήτησης των κατάλληλων προϊόντων, η παροχή προϊόντων, η εμπειρογνωσία στον τομέα των συναλλαγών και η αντιστοίχιση αγοραστών και πωλητών.

Ο όρος «επιγραμμική αγορά» ορίζεται στο άρθρο 4 σημείο 17 και αποσαφηνίζεται περαιτέρω στην αιτιολογική σκέψη 15. Περιγράφεται ως υπηρεσία που επιτρέπει σε καταναλωτές και εμπόρους να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με

εμπόρους, και αποτελεί τον τελικό προορισμό για τη σύναψη των εν λόγω συμβάσεων. Για παράδειγμα, ένας πάροχος υπηρεσιών όπως το *E-bay* μπορεί να θεωρηθεί επιγραμμική αγορά διότι επιτρέπει σε τρίτους να ανοίξουν καταστήματα στην πλατφόρμα του προκειμένου να διαθέτουν τα προϊόντα και τις υπηρεσίες τους επιγραμμικά σε καταναλωτές ή επιχειρήσεις. Στον ορισμό της επιγραμμικής αγοράς θεωρείται ότι εμπίπτουν επίσης τα διαδικτυακά καταστήματα εφαρμογών που διανέμουν εφαρμογές και προγράμματα λογισμικού, διότι επιτρέπουν στους υπεύθυνους ανάπτυξης εφαρμογών να πωλούν ή να διανέμουν τις υπηρεσίες τους σε καταναλωτές ή άλλες επιχειρήσεις. Ο ορισμός του άρθρου 4 σημείο 17 δεν καλύπτει, αντιθέτως, τους ενδιάμεσους σε υπηρεσίες τρίτων, όπως το *Skyscanner* και οι υπηρεσίες σύγκρισης τιμών, που ανακατευθύνουν τον χρήστη στον δικτυακό τόπο του εμπόρου όπου και συνάπτεται η σύμβαση για την υπηρεσία ή το προϊόν.

2. Πάροχος υπηρεσιών επιγραμμικής μηχανής αναζήτησης

Η έννοια της «επιγραμμικής μηχανής αναζήτησης» ορίζεται στο άρθρο 4 σημείο 18 και αποσαφηνίζεται περαιτέρω στην αιτιολογική σκέψη 16. Περιγράφεται ως ψηφιακή υπηρεσία που επιτρέπει στους χρήστες να εκτελούν αναζητήσεις κατ' αρχήν σε όλους τους ιστοχώρους ή σε ιστοχώρους συγκεκριμένης γλώσσας βάσει ερωτήματος για οποιοδήποτε θέμα. Δεν καλύπτονται οι λειτουργικές δυνατότητες αναζήτησης που περιορίζονται στην αναζήτηση εντός ενός δικτυακού τόπου μόνο και σε δικτυακούς τόπους σύγκρισης τιμών. Για παράδειγμα, ένα είδος μηχανής αναζήτησης όπως η μηχανή αναζήτησης του EUR LEX[34] δεν μπορεί να θεωρηθεί μηχανή αναζήτησης κατά την έννοια της οδηγίας, διότι η λειτουργία αναζήτησης που εκτελεί περιορίζεται στο περιεχόμενο του συγκεκριμένου δικτυακού τόπου.

3. Πάροχος υπηρεσιών νεφοϋπολογιστικής

Η υπηρεσία νεφοϋπολογιστικής ορίζεται στο άρθρο 4 σημείο 19 ως «ψηφιακή υπηρεσία που επιτρέπει την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων» και στην αιτιολογική σκέψη 17 παρέχονται περαιτέρω διευκρινίσεις για τους όρους «υπολογιστικοί πόροι» και «κλιμακοθετήσιμο και ελαστικό σύνολο».

Η νεφοϋπολογιστική μπορεί να περιγραφεί εν συντομία ως συγκεκριμένο είδος υπηρεσίας υπολογιστικής το οποίο χρησιμοποιεί κοινόχρηστους πόρους για την επεξεργασία δεδομένων κατά παραγγελία (on-demand). Στους εν λόγω κοινόχρηστους πόρους περιλαμβάνονται κάθε είδους στοιχεία υλισμικού ή λογισμικού (π.χ., δίκτυα, διακομιστές ή άλλες υποδομές, αποθήκευση, εφαρμογές και υπηρεσίες) τα οποία διατίθενται κατά παραγγελία στους χρήστες για την επεξεργασία δεδομένων. Ο όρος «κοινόχρηστος» χρησιμοποιείται για τους υπολογιστικούς πόρους όταν η ίδια φυσική υποδομή χρησιμοποιείται από πολλούς χρήστες για την επεξεργασία δεδομένων. Οι υπολογιστικοί πόροι μπορούν να οριστούν ως κοινόχρηστοι αν το συνολικό απόθεμα πόρων που χρησιμοποιεί ο πάροχος μπορεί να αυξηθεί ή να μειωθεί οποιαδήποτε στιγμή, ανάλογα με τις απαιτήσεις του χρήστη. Έτσι, μπορούν ενδεχομένως να προστεθούν ή να αφαιρεθούν ολόκληρα κέντρα δεδομένων ή μεμονωμένα στοιχεία ενός μόνο κέντρου δεδομένων, αν το συνολικό ύψος της υπολογιστικής ή αποθηκευτικής ισχύος χρήζει επικαιροποίησης. Ο όρος «ελαστικό σύνολο» μπορεί να

[34] Διαθέσιμη στον δικτυακό τόπο: http://eur-lex.europa.eu/homepage.html

περιγραφεί ως «οι μεταβολές του φόρτου εργασίας μέσω της αύξησης ή της μείωσης πόρων με αυτόματο τρόπο, έτσι ώστε σε κάθε χρονική στιγμή οι διαθέσιμοι πόροι να αντιστοιχούν όσο το δυνατόν περισσότερο στην τρέχουσα ζήτηση»[35].

Επί του παρόντος υπάρχουν τρία βασικά είδη μοντέλων υπηρεσίας νέφους που μπορεί να παρέχει ένας πάροχος:

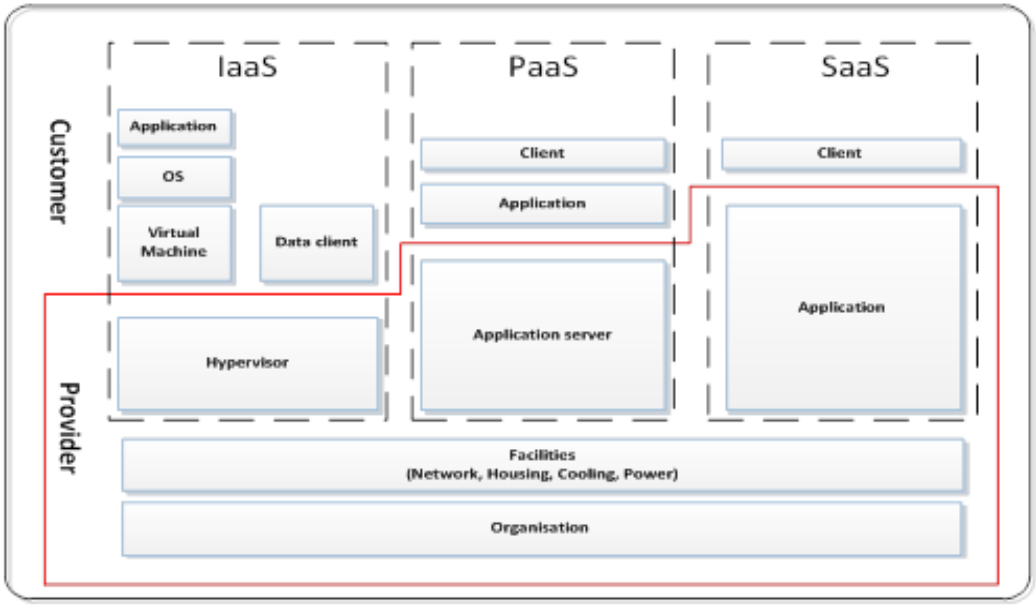
- Υποδομή ως υπηρεσία (Infrastructure as a Service - IaaS): Είδος υπηρεσίας νέφους στο πλαίσιο της οποίας οι δυνατότητες που παρέχονται στον πελάτη εμπίπτουν στην κατηγορία της υποδομής. Περιλαμβάνει την εικονική παροχή υπολογιστικών πόρων με τη μορφή υπηρεσιών υλισμικού, δικτύωσης και αποθήκευσης. Η IaaS αφορά συστήματα διακομιστών, αποθήκευσης, δικτύων, καθώς και λειτουργικά συστήματα. Παρέχει επιχειρηματική υποδομή στην οποία μια επιχείρηση μπορεί να αποθηκεύει τα δεδομένα της και να χρησιμοποιεί τις εφαρμογές που χρειάζεται για την καθημερινή της λειτουργία.

- Πλατφόρμα ως υπηρεσία (Platform as a Service - PaaS): Είδος υπηρεσίας νέφους στο πλαίσιο της οποίας οι δυνατότητες που παρέχονται στον πελάτη εμπίπτουν στην κατηγορία της πλατφόρμας. Περιλαμβάνει διαδικτυακές υπολογιστικές πλατφόρμες οι οποίες παρέχουν στις εταιρείες τη δυνατότητα να χρησιμοποιήσουν τις υφιστάμενες εφαρμογές ή να αναπτύξουν και να δοκιμάσουν νέες.

- Λογισμικό ως υπηρεσία (Software as a service - SaaS): Είδος υπηρεσίας νέφους στο πλαίσιο της οποίας οι δυνατότητες που παρέχονται στον πελάτη εμπίπτουν στην κατηγορία της εφαρμογής ή του λογισμικού που αναπτύσσεται και χρησιμοποιείται στο Διαδίκτυο. Οι υπηρεσίες νεφοϋπολογιστικής αυτού του είδους παρουσιάζουν το πλεονέκτημα ότι ο τελικός χρήστης δεν χρειάζεται να αγοράσει, να εγκαταστήσει και να διαχειριστεί λογισμικό, και επιπλέον ότι το λογισμικό είναι προσβάσιμο από οπουδήποτε μέσω διαδικτυακής σύνδεσης.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Ινστιτούτο Τεχνολογίας Καρλσρούης, «Elasticity in Cloud Computing: What It Is, and What It Is Not» (»Ελαστικότητα στη νεφοϋπολογιστική: τι είναι και τι δεν είναι»), έγγραφο διαθέσιμο στον δικτυακό τόπο: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Βλ. επίσης σελίδες 2-5 της ανακοίνωσης COM(2012) 529.

Σχήμα 5: Τα μοντέλα υπηρεσίας και οι βασικές παράμετροι της νεφοϋπολογιστικής



Αναλυτικές κατευθυντήριες γραμμές για συγκεκριμένους θεματικούς τομείς στο πλαίσιο του υπολογιστικού νέφους[36] και ένα έγγραφο καθοδήγησης για τις βασικές αρχές της νεφοϋπολογιστικής[37] έχουν δοθεί από τον ENISA.

4.4.2. Απαιτήσεις ασφάλειας

Σύμφωνα με το άρθρο 16 παράγραφος 1, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι πάροχοι ψηφιακών υπηρεσιών λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν οι εταιρείες κατά την παροχή των υπηρεσιών τους. Τα εν λόγω μέτρα ασφάλειας θα πρέπει να λαμβάνουν υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες και να συνεκτιμούν τα ακόλουθα πέντε στοιχεία: i) την ασφάλεια των συστημάτων και των εγκαταστάσεων· ii) τη διαχείριση συμβάντων· iii) τη διαχείριση της επιχειρησιακής συνέχειας· iv) την παρακολούθηση, τις επιθεωρήσεις και τις δοκιμές· v) τη συμμόρφωση με διεθνή πρότυπα.

Ως προς το θέμα αυτό, η Επιτροπή εξουσιοδοτείται δυνάμει του άρθρου 16 παράγραφος 8 να εκδίδει εκτελεστικές πράξεις που προσδιορίζουν περαιτέρω τα εν λόγω στοιχεία και διασφαλίζουν υψηλό επίπεδο εναρμόνισης για τους εν λόγω παρόχους υπηρεσιών. Η σχετική εκτελεστική πράξη αναμένεται να εκδοθεί από την Επιτροπή το φθινόπωρο του 2017. Επιπλέον, τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι οι πάροχοι ψηφιακών υπηρεσιών λαμβάνουν τα αναγκαία μέτρα για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων με σκοπό τη διασφάλιση της συνέχειας των υπηρεσιών τους.

[36] Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

[37] ENISA, *Cloud Security Guide for SMEs* (2015). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

4.4.3. Απαιτήσεις κοινοποίησης

Οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να διέπονται από την υποχρέωση κοινοποίησης των σοβαρών συμβάντων στις αρμόδιες αρχές ή τις CSIRT. Σύμφωνα με το άρθρο 16 παράγραφος 3 της οδηγίας ΑΔΠ, η απαίτηση κοινοποίησης που βαρύνει τους παρόχους ψηφιακών υπηρεσιών θα ενεργοποιείται όταν το συμβάν ασφαλείας έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας. Όσον αφορά τον προσδιορισμό του αντίκτυπου, στο άρθρο 16 παράγραφος 4 απαριθμούνται ειδικότερα πέντε παράμετροι τις οποίες πρέπει να λαμβάνουν υπόψη οι πάροχοι ψηφιακών υπηρεσιών. Ως προς το θέμα αυτό, η Επιτροπή εξουσιοδοτείται δυνάμει του άρθρου 16 παράγραφος 8 να εκδίδει εκτελεστικές πράξεις για τον περαιτέρω προσδιορισμό των εν λόγω παραμέτρων. Η περαιτέρω εξειδίκευση των εν λόγω παραμέτρων θα περιλαμβάνεται στην εκτελεστική πράξη την οποία σκοπεύει να εκδώσει η Επιτροπή το φθινόπωρο, όπου θα προσδιορίζονται τα σχετικά με την ασφάλεια στοιχεία που αναφέρονται στο σημείο 4.4.2.

4.4.4. Ρυθμιστική προσέγγιση βάσει κινδύνου

Το άρθρο 17 προβλέπει ότι οι πάροχοι ψηφιακών υπηρεσιών υπόκεινται σε εκ των υστέρων εποπτικό έλεγχο από τις αρμόδιες εθνικές αρχές. Τα κράτη μέλη οφείλουν να διασφαλίζουν την ανάληψη δράσης από τις αρμόδιες αρχές, όταν τους παρέχονται στοιχεία που αποδεικνύουν ότι πάροχος ψηφιακών υπηρεσιών δεν συμμορφώνεται με τις απαιτήσεις του άρθρου 16 της οδηγίας.

Επιπλέον, σύμφωνα με το άρθρο 16 παράγραφοι 8 και 9, η Επιτροπή εξουσιοδοτείται να εκδίδει εκτελεστικές πράξεις σχετικά με τις απαιτήσεις κοινοποίησης και ασφάλειας οι οποίες θα ενισχύσουν το επίπεδο εναρμόνισης για τους παρόχους ψηφιακών υπηρεσιών. Ακόμη, σύμφωνα με το άρθρο 16 παράγραφος 10, τα κράτη μέλη δεν επιτρέπεται να επιβάλλουν οποιεσδήποτε περαιτέρω απαιτήσεις ασφάλειας και κοινοποίησης στους παρόχους ψηφιακών υπηρεσιών πέραν εκείνων που προβλέπονται στην οδηγία ΑΔΠ, εξαιρουμένων των περιπτώσεων στις οποίες η λήψη τέτοιων μέτρων είναι αναγκαία για τη διαφύλαξη των ουσιωδών κρατικών λειτουργιών τους, και ιδίως για τη διαφύλαξη της εθνικής ασφάλειας, καθώς και για τη διευκόλυνση της διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων.

Τέλος, λαμβάνοντας υπόψη τη διασυνοριακή φύση των παρόχων ψηφιακών υπηρεσιών, η οδηγία δεν ακολουθεί το μοντέλο των πολλών παράλληλων δικαιοδοσιών, αλλά μια προσέγγιση που βασίζεται στο κριτήριο της κύριας εγκατάστασης της εταιρείας στην ΕΕ[38]. Με τη συγκεκριμένη προσέγγιση, οι πάροχοι ψηφιακών υπηρεσιών διέπονται από μία και μόνη δέσμη κανόνων, ενώ για την εποπτεία τους υπεύθυνη είναι μία αρμόδια αρχή, γεγονός που είναι ιδιαίτερα σημαντικό καθώς πολλοί πάροχοι ψηφιακών υπηρεσιών προσφέρουν τις υπηρεσίες τους σε πολλά κράτη μέλη ταυτόχρονα. Η εφαρμογή της εν λόγω προσέγγισης ελαχιστοποιεί τις υποχρεώσεις συμμόρφωσης που βαρύνουν τους παρόχους ψηφιακών υπηρεσιών και διασφαλίζει την εύρυθμη λειτουργία της ψηφιακής ενιαίας αγοράς.

[38] Βλ. ιδίως το άρθρο 18 της οδηγίας.

4.4.5. Δικαιοδοσία

Όπως επεξηγείται ανωτέρω, σύμφωνα με το άρθρο 18 παράγραφος 1 της οδηγίας ΑΔΠ, ένας πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο έχει την κύρια εγκατάστασή του. Όταν ένας πάροχος ψηφιακών υπηρεσιών προσφέρει υπηρεσίες στην Ένωση χωρίς να είναι εγκατεστημένος στο έδαφος της ΕΕ, το άρθρο 18 παράγραφος 2 επιβάλλει στον πάροχο ψηφιακών υπηρεσιών την υποχρέωση να ορίζει αντιπρόσωπο στην Ένωση. Σε αυτήν την περίπτωση, ο πάροχος ψηφιακών υπηρεσιών υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο αντιπρόσωπος Όταν ο πάροχος ψηφιακών υπηρεσιών προσφέρει υπηρεσίες σε ένα κράτος μέλος χωρίς να έχει ορίσει αντιπρόσωπο στην ΕΕ, το κράτος μέλος μπορεί καταρχήν να λάβει μέτρα κατά του παρόχου ψηφιακών υπηρεσιών καθώς ο τελευταίος παραβιάζει τις υποχρεώσεις που τον βαρύνουν δυνάμει της οδηγίας.

4.4.6. Εξαίρεση των παρόχων ψηφιακών υπηρεσιών περιορισμένης κλίμακας από το πεδίο εφαρμογής των απαιτήσεων ασφάλειας και κοινοποίησης συμβάντων

Σύμφωνα με το άρθρο 16 παράγραφος 11, οι πάροχοι ψηφιακών υπηρεσιών που είναι πολύ μικρές ή μικρές επιχειρήσεις κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής39 εξαιρούνται από το πεδίο εφαρμογής των απαιτήσεων ασφάλειας και κοινοποίησης του άρθρου 16. Αυτό σημαίνει ότι στις εν λόγω απαιτήσεις δεν υπόκεινται οι επιχειρήσεις που απασχολούν λιγότερους από 50 εργαζομένους και των οποίων ο ετήσιος κύκλος εργασιών και/ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 10 εκατ. EUR. Για τον καθορισμό του μεγέθους της οντότητας, δεν έχει σημασία αν η υπό εξέταση εταιρεία παρέχει μόνο ψηφιακές υπηρεσίες κατά την έννοια της οδηγίας ΑΔΠ ή και άλλες υπηρεσίες.

5. Σχέση μεταξύ της οδηγίας ΑΔΠ και λοιπής νομοθεσίας

Η παρούσα ενότητα πραγματεύεται τις διατάξεις περί *lex specialis* της οδηγίας ΑΔΠ, ήτοι το άρθρο 1 παράγραφος 7, επεξηγώντας τα τρία παραδείγματα *lex specialis* που έχουν εκτιμηθεί μέχρι στιγμής από την Επιτροπή, και αποσαφηνίζοντας τις απαιτήσεις ασφάλειας και κοινοποίησης που διέπουν τους παρόχους τηλεπικοινωνιακών υπηρεσιών και υπηρεσιών εμπιστοσύνης.

5.1. Οδηγία ΑΔΠ, άρθρο 1 παράγραφος 7: Η διάταξη περί *lex specialis*

Σύμφωνα με το άρθρο 1 παράγραφος 7 της οδηγίας ΑΔΠ, οι διατάξεις της οδηγίας ΑΔΠ σχετικά με τις απαιτήσεις ασφάλειας και/ή κοινοποίησης για τους παρόχους ψηφιακών υπηρεσιών ή τους φορείς εκμετάλλευσης βασικών υπηρεσιών δεν εφαρμόζονται εάν υφίσταται τομεακή νομοθεσία της ΕΕ η οποία προβλέπει απαιτήσεις ασφάλειας και/ή κοινοποίησης τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που θεσπίζονται στην οδηγία ΑΔΠ. Τα κράτη μέλη οφείλουν να λάβουν υπόψη το άρθρο 1 παράγραφος 7 κατά τη μεταφορά της οδηγίας ΑΔΠ στα εθνικά τους δίκαια και να υποβάλουν πληροφορίες στην Επιτροπή σχετικά με την εφαρμογή των διατάξεων περί *lex specialis*.

[39] ΕΕ L 24 της 20.5.2003, σ. 36

Μεθοδολογία

Κατά την αξιολόγηση της ισοδυναμίας μιας τομεακής νομικής πράξης με τις συναφείς διατάξεις της οδηγίας ΑΔΠ, θα πρέπει να ελέγχεται με ιδιαίτερη προσοχή εάν στις υποχρεώσεις ασφάλειας που προβλέπει η τομεακή νομοθεσία περιλαμβάνονται μέτρα τα οποία διασφαλίζουν την ασφάλεια συστημάτων δικτύου και πληροφοριών κατά την έννοια του άρθρου 4 παράγραφος 2 της οδηγίας ΑΔΠ.

Όσον αφορά τις απαιτήσεις κοινοποίησης, το άρθρο 14 παράγραφος 3 και το άρθρο 16 παράγραφος 3 της οδηγίας ΑΔΠ προβλέπουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών οφείλουν να κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια αρχή ή στην CSIRT κάθε συμβάν με σοβαρό/σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που προσφέρουν. Στο σημείο αυτό πρέπει να δίδεται ιδιαίτερη προσοχή στην υποχρέωση των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών να περιλαμβάνουν στην κοινοποίηση πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσει τον τυχόν διασυνοριακό αντίτυπο του συμβάντος ασφαλείας.

Επί του παρόντος δεν υφίσταται τομεακή νομοθεσία για την κατηγορία των παρόχων ψηφιακών υπηρεσιών η οποία να προβλέπει απαιτήσεις ασφάλειας και κοινοποίησης συγκρίσιμες με εκείνες του άρθρου 16 της οδηγίας ΑΔΠ που να μπορούν να ληφθούν υπόψη κατά την εφαρμογή του άρθρου 1 παράγραφος 7 της οδηγίας ΑΔΠ[40].

Όσον αφορά τους φορείς εκμετάλλευσης βασικών υπηρεσιών, ο χρηματοπιστωτικός τομέας και ιδίως οι τομείς των τραπεζών και των υποδομών χρηματοπιστωτικών αγορών που αναφέρονται στα σημεία 3 και 4 του παραρτήματος ΙΙ υπόκεινται ήδη σε απαιτήσεις ασφάλειας και/ή κοινοποίησης που απορρέουν από τομεακή νομοθεσία της ΕΕ. Αυτό οφείλεται στο γεγονός ότι η ασφάλεια και η αρτιότητα των πληροφοριακών συστημάτων και των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν τα χρηματοπιστωτικά ιδρύματα αποτελεί καίρια συνιστώσα των απαιτήσεων περί λειτουργικού κινδύνου που διέπουν τα χρηματοπιστωτικά ιδρύματα δυνάμει της νομοθεσίας της ΕΕ.

Παραδείγματα

i) Οδηγία για τις υπηρεσίες πληρωμών 2

Όσον αφορά τον τραπεζικό τομέα, και ειδικότερα την παροχή υπηρεσιών πληρωμών από πιστωτικά ιδρύματα κατά την έννοια του άρθρου 4 σημείο 1) του κανονισμού (ΕΕ) 575/2013, απαιτήσεις ασφάλειας και κοινοποίησης προβλέπονται αντίστοιχα στα άρθρα 95 και 96 της οδηγίας για τις υπηρεσίες πληρωμών 2 (PSD 2)[41].

[40] Με την επιφύλαξη της γνωστοποίησης παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που καλύπτεται από το άρθρο 33 του γενικού κανονισμού για την προστασία δεδομένων.
[41] Οδηγία (ΕΕ) 2015/2366, ΕΕ L 337 της 23.12.2015, σ. 35

Πιο συγκεκριμένα, το άρθρο 95 παράγραφος 1 επιβάλλει στους παρόχους υπηρεσιών πληρωμών την υποχρέωση να λαμβάνουν κατάλληλα μέτρα μείωσης κινδύνων και μηχανισμούς ελέγχου για τη διαχείριση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας που σχετίζονται με τις υπηρεσίες πληρωμών τις οποίες παρέχουν. Στο πλαίσιο των εν λόγω μέτρων, οι πάροχοι υπηρεσιών πληρωμών θα πρέπει να θεσπίζουν και να διατηρούν αποτελεσματικές διαδικασίες διαχείρισης συμβάντων, μεταξύ άλλων για τον εντοπισμό και την ταξινόμηση των μειζόνων συμβάντων που άπτονται της λειτουργίας και της ασφάλειας. Στις αιτιολογικές σκέψεις 95 και 96 της οδηγίας PSD 2 αποσαφηνίζεται περαιτέρω η φύση των εν λόγω μέτρων ασφαλείας. Από τις συγκεκριμένες διατάξεις προκύπτει σαφώς ότι τα προβλεπόμενα μέτρα αποσκοπούν στη διαχείριση των κινδύνων ασφάλειας που σχετίζονται με τα συστήματα δικτύου και πληροφοριών τα οποία χρησιμοποιούνται για την παροχή υπηρεσιών πληρωμών. Είναι δυνατό επομένως να συναχθεί ότι οι εν λόγω απαιτήσεις ασφαλείας είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις αντίστοιχες διατάξεις του άρθρου 14 παράγραφοι 1 και 2 της οδηγίας ΑΔΠ.

Όσον αφορά τις απαιτήσεις κοινοποίησης, το άρθρο 96 παράγραφος 1 της οδηγίας PSD 2 προβλέπει την υποχρέωση των παρόχων υπηρεσιών πληρωμών να γνωστοποιούν, χωρίς υπαίτια καθυστέρηση, στην αρμόδια αρχή σοβαρά συμβάντα ασφαλείας. Επιπλέον, το άρθρο 96 παράγραφος 2 της οδηγίας PSD 2, το οποίο είναι συγκρίσιμο με το άρθρο 14 παράγραφος 5 της οδηγίας ΑΔΠ, επιβάλλει στην αρμόδια αρχή την υποχρέωση να ενημερώνει τις αρμόδιες αρχές άλλων κρατών μελών, εφόσον το συμβάν τα αφορά. Η εν λόγω υποχρέωση προϋποθέτει ταυτόχρονα ότι στην αναφορά συμβάντων ασφαλείας πρέπει να περιλαμβάνονται πληροφορίες που επιτρέπουν στις αρχές να προσδιορίζουν τον διασυνοριακό αντίκτυπο ενός συμβάντος. Το άρθρο 96 παράγραφος 3 στοιχείο α) της οδηγίας PSD 2 εξουσιοδοτεί σχετικά την Ευρωπαϊκή Αρχή Τραπεζών (ΕΑΤ) να καταρτίσει, σε συνεργασία με την Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ), κατευθυντήριες γραμμές για το ακριβές περιεχόμενο και τη μορφή της κοινοποίησης.

Συνάγεται επομένως ότι, σύμφωνα με το άρθρο 1 παράγραφος 7 της οδηγίας ΑΔΠ, όσον αφορά την παροχή υπηρεσιών πληρωμών από πιστωτικά ιδρύματα θα πρέπει να εφαρμόζονται οι απαιτήσεις ασφάλειας και κοινοποίησης των άρθρων 95 και 96 της οδηγίας PSD 2 αντί των αντίστοιχων διατάξεων του άρθρου 14 της οδηγίας ΑΔΠ.

ii) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4 Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών.

Όσον αφορά τις υποδομές χρηματοπιστωτικών αγορών, ο κανονισμός (ΕΕ) αριθ. 648/2012, σε συνδυασμό με τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) αριθ. 153/2013 της Επιτροπής, περιέχει διατάξεις που προβλέπουν απαιτήσεις ασφαλείας για τους κεντρικούς αντισυμβαλλομένους οι οποίες μπορούν να θεωρηθούν ως *lex specialis.* Συγκεκριμένα, οι προαναφερθείσες νομικές πράξεις προβλέπουν τεχνικά και οργανωτικά μέτρα σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών τα οποία είναι περισσότερο λεπτομερή σε σύγκριση με τις απαιτήσεις του άρθρου 14 παράγραφοι 1 και 2 της οδηγίας ΑΔΠ. Είναι,

συνεπώς, δυνατό να θεωρηθεί ότι πληρούν τις απαιτήσεις του άρθρου 1 παράγραφος 7 της οδηγίας ΑΔΠ όσον αφορά τις απαιτήσεις ασφαλείας.

Πιο συγκεκριμένα, το άρθρο 26 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 648/2012 αναφέρει ότι η οντότητα θα πρέπει να «*διαθέτει άρτιο πλαίσιο διακυβέρνησης, που περιλαμβάνει σαφή οργανωτική δομή με ευκρινείς, διαφανείς και συνεπείς γραμμές ευθύνης, αποτελεσματικές διαδικασίες εντοπισμού, διαχείρισης, παρακολούθησης και αναφοράς των κινδύνων στους οποίους εκτίθεται ή ενδέχεται να εκτεθεί, καθώς και επαρκείς μηχανισμούς εσωτερικού ελέγχου, περιλαμβανομένων ορθών διοικητικών και λογιστικών διαδικασιών.*» Το άρθρο 26 παράγραφος 3 ορίζει ότι η οργανωτική δομή πρέπει να διασφαλίζει τη συνέχεια και την εύρυθμη λειτουργία των υπηρεσιών και των δραστηριοτήτων χρησιμοποιώντας κατάλληλα και ανάλογα συστήματα, πόρους και διαδικασίες.

Επιπλέον, το άρθρο 26 παράγραφος 6 διευκρινίζει ότι ο κεντρικός αντισυμβαλλόμενος πρέπει να διατηρεί «*συστήματα τεχνολογίας των πληροφοριών κατάλληλα για τη διαχείριση της πολυπλοκότητας, της ποικιλίας και των ειδών των παρεχόμενων υπηρεσιών και των ασκούμενων δραστηριοτήτων, ούτως ώστε να κατοχυρώνονται υψηλά επίπεδα ασφαλείας, καθώς και η ακεραιότητα και η εμπιστευτικότητα των διατηρούμενων πληροφοριών».* Ακόμη, το άρθρο 34 παράγραφος 1 επιβάλλει στον κεντρικό αντισυμβαλλόμενο την υποχρέωση να διαμορφώνει, εφαρμόζει και διατηρεί κατάλληλη πολιτική αδιάλειπτης λειτουργίας και σχέδιο αποκατάστασης λειτουργίας μετά από καταστροφή που θα διασφαλίζει την έγκαιρη αποκατάσταση των εργασιών.

Οι εν λόγω υποχρεώσεις εξειδικεύονται περαιτέρω στον κατ' εξουσιοδότηση κανονισμό (ΕΕ) αριθ. 153/2013 της Επιτροπής, της 19ης Δεκεμβρίου 2012, για την εφαρμογή του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα σχετικά με τις απαιτήσεις για τους κεντρικούς αντισυμβαλλομένους[42]. Συγκεκριμένα, το άρθρο 4 του εν λόγω κανονισμού επιβάλλει στους κεντρικούς αντισυμβαλλόμενους την υποχρέωση να αναπτύσσουν κατάλληλα εργαλεία διαχείρισης κινδύνου ώστε να είναι σε θέση να διαχειρίζονται και να αναφέρουν όλους τους σχετικούς κινδύνους και προσδιορίζει περαιτέρω το είδος των μέτρων (π.χ.: χρησιμοποίηση άρτιων συστημάτων πληροφόρησης και ελέγχου του κινδύνου, διαθεσιμότητα απαραίτητων πόρων, εμπειρογνωμοσύνη και πρόσβαση σε όλες τις σχετικές πληροφορίες για την υπηρεσία διαχείρισης κινδύνου, διαθεσιμότητα επαρκών μηχανισμών εσωτερικού ελέγχου, όπως ορθές διοικητικές και λογιστικές διαδικασίες που συνδράμουν το συμβούλιο του κεντρικού αντισυμβαλλομένου στην παρακολούθηση και εκτίμηση της επάρκειας και αποτελεσματικότητας των πολιτικών, των διαδικασιών και των συστημάτων διαχείρισης κινδύνου που εφαρμόζει ο κεντρικός αντισυμβαλλόμενος).

Επιπλέον, το άρθρο 9 αναφέρεται ρητώς στην ασφάλεια των συστημάτων τεχνολογίας των πληροφοριών και επιβάλλει την υποχρέωση λήψης συγκεκριμένων τεχνικών και οργανωτικών μέτρων με γνώμονα τη διατήρηση άρτιου πλαισίου ασφαλείας των πληροφοριών για τη διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια των

[42] ΕΕ L 52 της 23.2.2013, σ. 41

τεχνολογιών πληροφοριών. Στα μέτρα αυτά θα πρέπει να περιλαμβάνονται μηχανισμοί και διαδικασίες που διασφαλίζουν τη διαθεσιμότητα των υπηρεσιών και την προστασία της αυθεντικότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

iii) Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ[43]

Όσον αφορά τους τόπους διαπραγμάτευσης, το άρθρο 48 παράγραφος 1 της οδηγίας 2014/65/ΕΕ επιβάλλει στους διαχειριστές αγοράς την υποχρέωση να διασφαλίζουν τη συνέχιση των υπηρεσιών της σε περίπτωση αστοχίας των συστημάτων συναλλαγών. Αυτή η γενική υποχρέωση εξειδικεύτηκε και συμπληρώθηκε πρόσφατα περαιτέρω με τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2017/584 της Επιτροπής[44], της 14ης Ιουλίου 2016, για τη συμπλήρωση της οδηγίας 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά ρυθμιστικά τεχνικά πρότυπα τα οποία προσδιορίζουν οργανωτικές απαιτήσεις για τόπους διαπραγμάτευσης[45]. Συγκεκριμένα, το άρθρο 23 παράγραφος 1 του εν λόγω κανονισμού ορίζει ότι οι τόποι διαπραγμάτευσης εφαρμόζουν διαδικασίες και ρυθμίσεις φυσικής και ηλεκτρονικής ασφάλειας, οι οποίες έχουν σχεδιαστεί για να προστατεύουν τα συστήματά τους από κατάχρηση ή μη εξουσιοδοτημένη πρόσβαση και να διασφαλίζουν την ακεραιότητα των δεδομένων. Τα μέτρα αυτά θα πρέπει να επιτρέπουν την πρόληψη ή την ελαχιστοποίηση του κινδύνου επιθέσεων κατά πληροφοριακών συστημάτων.

Το άρθρο 23 παράγραφος 2 ορίζει περαιτέρω ότι τα μέτρα και οι ρυθμίσεις που λαμβάνονται από τους διαχειριστές αγοράς θα πρέπει να επιτρέπουν τον άμεσο εντοπισμό και τη διαχείριση των κινδύνων που σχετίζονται με τυχόν μη εξουσιοδοτημένη πρόσβαση, παρεμβολές στα συστήματα που εμποδίζουν σημαντικά ή διακόπτουν τη λειτουργία πληροφοριακών συστημάτων και παρεμβολές στα δεδομένα που πλήττουν τη διαθεσιμότητα, την ακεραιότητα ή την αυθεντικότητα των δεδομένων. Επιπλέον, το άρθρο 15 του κανονισμού επιβάλλει στους τόπους διαπραγμάτευσης την υποχρέωση να διαθέτουν αποτελεσματικές ρυθμίσεις επιχειρησιακής συνέχειας για τη διασφάλιση της επαρκούς σταθερότητας των συστημάτων και την αντιμετώπιση συμβάντων δυσλειτουργίας. Συγκεκριμένα, τα μέτρα αυτά θα πρέπει να παρέχουν στον διαχειριστή αγοράς τη δυνατότητα να συνεχίζει τις συναλλαγές εντός δύο ωρών ή περίπου σε δύο ώρες από οποιοδήποτε συμβάν δυσλειτουργίας και ταυτόχρονα να διασφαλίζουν ότι ο όγκος απολεσθέντων δεδομένων είναι σχεδόν μηδενικός.

Το άρθρο 16 ορίζει περαιτέρω ότι τα μέτρα που έχουν καθοριστεί για την αντιμετώπιση και διαχείριση συμβάντων δυσλειτουργίας θα πρέπει να περιέχονται στο σχέδιο επιχειρησιακής συνέχειας των τόπων διαπραγμάτευσης, και προβλέπει επιπλέον συγκεκριμένα στοιχεία τα οποία πρέπει να λαμβάνει υπόψη ο διαχειριστής αγοράς κατά την έγκριση του σχεδίου επιχειρησιακής συνέχειας (π.χ. δημιουργία ειδικής επιχειρησιακής ομάδας ασφάλειας,

[43] ΕΕ L 173 της 12.6.2014, σ. 349
[44] ΕΕ L 87 της 31.3.2017, σ. 350
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

διενέργεια και περιοδική επανεξέταση εκτίμησης επιπτώσεων για τον προσδιορισμό των κινδύνων).

Ως προς το περιεχόμενο των εν λόγω μέτρων ασφαλείας, προκύπτει ότι αποσκοπούν στη διαχείριση και αντιμετώπιση του κινδύνου που σχετίζεται με τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα και το απόρρητο των δεδομένων ή των παρεχόμενων υπηρεσιών. Είναι δυνατό επομένως να συναχθεί ότι η προαναφερθείσα τομεακή νομοθεσία της ΕΕ περιέχει υποχρεώσεις ασφαλείας που είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις αντίστοιχες υποχρεώσεις του άρθρου 14 παράγραφοι 1 και 2 της οδηγίας ΑΔΠ.

5.2 Οδηγία ΑΔΠ, άρθρο 1 παράγραφος 3: Πάροχοι τηλεπικοινωνιακών υπηρεσιών και υπηρεσιών εμπιστοσύνης

Σύμφωνα με το άρθρο 1 παράγραφος 3, οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στην οδηγία ΑΔΠ δεν εφαρμόζονται σε παρόχους που υπόκεινται στις απαιτήσεις των άρθρων 13α και 13β της οδηγίας 2002/21/ΕΚ. Τα άρθρα 13α και 13β της οδηγίας 2002/21/ΕΚ εφαρμόζονται σε επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό. Συνεπώς, όσον αφορά την παροχή δημόσιων δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό, η εταιρεία πρέπει να συμμορφώνεται με τις απαιτήσεις ασφάλειας και κοινοποίησης της οδηγίας 2002/21/ΕΚ.

Αν, όμως, η ίδια εταιρεία παρέχει και άλλες υπηρεσίες, όπως ψηφιακές υπηρεσίες (π.χ. υπηρεσίες νεφοϋπολογιστικής ή επιγραμμικής αγοράς) που αναφέρονται στο παράρτημα ΙΙΙ της οδηγίας ΑΔΠ ή υπηρεσίες όπως το σύστημα ονομάτων χώρου (DNS) ή το σημείο ανταλλαγής κίνησης διαδικτύου (IXP) σύμφωνα με το παράρτημα ΙΙ σημείο 7 της οδηγίας ΑΔΠ, τότε η εταιρεία θα υπόκειται στις απαιτήσεις ασφάλειας και κοινοποίησης της οδηγίας ΑΔΠ όσον αφορά την παροχή των συγκεκριμένων αυτών υπηρεσιών. Θα πρέπει να σημειωθεί ότι επειδή οι πάροχοι υπηρεσιών που αναφέρονται στο παράρτημα ΙΙ σημείο 7 εμπίπτουν στην κατηγορία των φορέων εκμετάλλευσης βασικών υπηρεσιών, τα κράτη μέλη οφείλουν να διεξαγάγουν τη διαδικασία προσδιορισμού που προβλέπεται στο άρθρο 5 παράγραφος 2 και να προσδιορίσουν χωριστά για κάθε πάροχο υπηρεσιών DNS, IXP ή TLD εάν θα πρέπει να συμμορφωθεί με τις απαιτήσεις της οδηγίας ΑΔΠ. Αυτό σημαίνει ότι, αφού ολοκληρωθεί η διαδικασία προσδιορισμού, η υποχρέωση συμμόρφωσης με τις απαιτήσεις της οδηγίας ΑΔΠ θα βαρύνει μόνο τους παρόχους DNS, IXP ή TLD που πληρούν τα κριτήρια του άρθρου 5 παράγραφος 2 της οδηγίας ΑΔΠ.

Το άρθρο 1 παράγραφος 3 ορίζει ακόμη ότι οι απαιτήσεις ασφάλειας και κοινοποίησης της οδηγίας ΑΔΠ δεν εφαρμόζονται ούτε σε παρόχους υπηρεσιών εμπιστοσύνης που υπόκεινται σε παρεμφερείς απαιτήσεις δυνάμει του άρθρου 19 του κανονισμού (ΕΕ) αριθ. 910/2014.

6. Δημοσιευμένα έγγραφα εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο

	Κράτος μέλος	Τίτλος στρατηγικής και διαθέσιμοι σύνδεσμοι
1	Αυστρία	*Austrian Cybersecurity Strategy (Η στρατηγική της Αυστρίας για την ασφάλεια στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Βέλγιο	*Securing Cyberspace (Ενίσχυση της ασφάλειας στον κυβερνοχώρο)* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Βουλγαρία	*Cyber Resilient Bulgaria 2020 (Ενίσχυση της ανθεκτικότητας της Βουλγαρίας στον κυβερνοχώρο 2020)* (2016) http://www.cyberbg.eu/ (BG)
4	Κροατία	*The national cyber security strategy of the republic of Croatia (Η εθνική στρατηγική της Δημοκρατίας της Κροατίας για την ασφάλεια στον κυβερνοχώρο)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Τσεχική Δημοκρατία	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020 (Η εθνική στρατηγική της Τσεχικής Δημοκρατίας για την ασφάλεια στον κυβερνοχώρο για την περίοδο από το 2015 έως το 2020)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Κύπρος	*Cybersecurity Strategy of the Republic of Cyprus (Η στρατηγική της Κυπριακής Δημοκρατίας για την ασφάλεια στον κυβερνοχώρο)* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Δανία	*The Danish Cyber and Information Security Strategy (Η στρατηγική της Δανίας για την ασφάλεια των πληροφοριών και την ασφάλεια στον κυβερνοχώρο)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Εσθονία	*Cyber Security Strategy (Στρατηγική για την ασφάλεια στον κυβερνοχώρο)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)

9	Φινλανδία	*Finland´s Cyber security Strategy (Η στρατηγική της Φινλανδίας για την ασφάλεια στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Γαλλία	*French national digital security strategy (Η εθνική στρατηγική της Γαλλίας για την ψηφιακή ασφάλεια)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Ιρλανδία	*National Cyber Security Strategy 2015-2017 (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο 2015-2017)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Ιταλία	*National Strategic Framework for Cyberspace Security (Εθνικό στρατηγικό πλαίσιο για την ασφάλεια στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Γερμανία	*Η στρατηγική της Γερμανίας για την ασφάλεια στον κυβερνοχώρο)* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ουγγαρία	*National Cyber Security Strategy of Hungary (Η εθνική στρατηγική της Ουγγαρίας για την ασφάλεια στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Λετονία	*Cyber Security Strategy of Latvia 2014–2018 (Η στρατηγική της Λετονίας για την ασφάλεια στον κυβερνοχώρο 2014–2018)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Λιθουανία	*The programme for the development of electronic information security (cyber-security) for 2011–2019 (Το πρόγραμμα για την ανάπτυξη της ασφάλειας των ηλεκτρονικών πληροφοριών (ασφάλεια στον κυβερνοχώρο) 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Λουξεμβούργο	*National Cybersecurity Strategy II (2015) (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)

18	Μάλτα	*National Cyber Security Strategy Green Paper (Η πράσινη βίβλος της εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Κάτω Χώρες	*National Cyber Security Strategy 2 (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο 2)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Πολωνία	*Cyberspace Protection Policy of the Republic of Poland (Η πολιτική της Δημοκρατίας της Πολωνίας για την προστασία στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Ρουμανία	*Η στρατηγική της Ρουμανίας για την ασφάλεια στον κυβερνοχώρο* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Πορτογαλία	*National Cyberspace Security Strategy (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Σλοβακική Δημοκρατία	*Cyber Security Concept of the Slovak Republic for 2015 – 2020 (Η προσέγγιση της Σλοβακικής Δημοκρατίας για την ασφάλεια στον κυβερνοχώρο)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Σλοβενία	*Cyber Security Strategy establishing a system to ensure a high level of cyber security (Στρατηγική για την ασφάλεια στον κυβερνοχώρο - Θέσπιση συστήματος για τη διασφάλιση υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο)* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Ισπανία	*National Cyber Security Strategy (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Σουηδία	*The Swedish National Cybersecurity Strategy (Η εθνική στρατηγική της Σουηδίας για την ασφάλεια στον κυβερνοχώρο)* (2017)

		http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Ηνωμένο Βασίλειο	*National Cyber Security Strategy 2016-2021 (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο 2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Κατάλογος ορθών πρακτικών και συστάσεων που έχουν εκδοθεί από τον ENISA.

Για την αντιμετώπιση συμβάντων

- ✓ Στρατηγικές αντιμετώπισης συμβάντων και συνεργασίας σε περιπτώσεις κρίσεων στον κυβερνοχώρο[46]

Για τη διαχείριση συμβάντων

- ✓ Έργο για την αυτοματοποίηση της διαχείρισης συμβάντων[47]
- ✓ Οδηγός ορθών πρακτικών διαχείρισης συμβάντων[48]

Για την κατηγοριοποίηση και την ταξινόμηση συμβάντων

- ✓ Επισκόπηση υφιστάμενων ταξινομιών[49]
- ✓ Οδηγός ορθών πρακτικών χρήσης των ταξινομιών για την πρόληψη και τον εντοπισμό συμβάντων[50]

Για το επίπεδο ωριμότητας των CSIRT

- ✓ Προκλήσεις για τις εθνικές CSIRT στην Ευρώπη το 2016: Μελέτη για το επίπεδο ωριμότητας των CSIRT[51]
- ✓ Μελέτη για το επίπεδο ωριμότητας των CSIRT – Διαδικασία αξιολόγησης[52]
- ✓ Κατευθυντήριες γραμμές προς εθνικές και κρατικές CSIRT για τους τρόπους αξιολόγησης του επιπέδου ωριμότητας[53]

Για την ανάπτυξη ικανοτήτων και την κατάρτιση των CSIRT

- ✓ Οδηγός ορθής πρακτικής για την ανάπτυξη μεθόδων κατάρτισης[54]

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[47] Για περισσότερες πληροφορίες, βλέπε: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

[48] ENISA, *Good Practice Guide for Incident Management* (2010). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[49] Για περισσότερες πληροφορίες, βλέπε: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο: https://www.enisa.europa.eu/publications/csirt-capabilities

[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Το έγγραφο είναι διαθέσιμο στον δικτυακό τόπο:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

Για περισσότερες πληροφορίες σχετικά με τις υφιστάμενες CSIRT στην Ευρώπη - Επισκόπηση των CSIRT ανά χώρα[55]

[55] Για περισσότερες πληροφορίες, βλέπε: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map