ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 7.2.2013
SWD(2013) 31 final

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΤΟΥ ΑΝΤΙΚΤΥΠΟΥ

που συνοδεύει το έγγραφο

Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

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

{COM(2013) 48 final}
{SWD(2013) 32 final}

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΤΟΥ ΑΝΤΙΚΤΥΠΟΥ

που συνοδεύει το έγγραφο

Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

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

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα εκτίμηση του αντίκτυπου αφορά τις επιλογές πολιτικής για τη βελτίωση της ασφάλειας του διαδικτύου και άλλων δικτύων και συστημάτων πληροφοριών που υποστηρίζουν υπηρεσίες οι οποίες εξυπηρετούν την λειτουργία της κοινωνίας μας (π.χ. δημόσια διοίκηση, χρηματοδοτικός και τραπεζικός τομέας, ενέργεια, μεταφορές, υγεία και ορισμένες διαδικτυακές υπηρεσίες που καθιστούν δυνατή τη διεξαγωγή βασικών οικονομικών και κοινωνικών διεργασιών, όπως οι πλατφόρμες ηλ-εμπορίου και τα κοινωνικά δίκτυα). Το θέμα αυτό αναφέρεται ως ασφάλεια δικτύων και πληροφοριών (NIS/ΑΔΠ).

2. ΠΛΑΙΣΙΟ ΠΟΛΙΤΙΚΗΣ

Η αυξανόμενη σημασία της ΑΔΠ για τις οικονομίες και τις κοινωνίες μας αναγνωρίστηκε για πρώτη φορά από την Επιτροπή το 2001. Για να διασφαλιστεί υψηλό και αποτελεσματικό επίπεδο ασφάλειας δικτύων και πληροφοριών στην ΕΕ, η Ευρωπαϊκή Κοινότητα αποφάσισε το 2004 τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Η προσέγγιση που ακολούθησε έως τώρα η Ευρωπαϊκή Ένωση στο πεδίο της ασφάλειας δικτύων και πληροφοριών συνίστατο κυρίως στη θέσπιση μιας σειράς σχεδίων δράσης και στρατηγικών που παρακινούν τα κράτη μέλη να αυξήσουν τις οικείες ικανότητες ΑΔΠ και να συνεργαστούν για την πάταξη των διασυνοριακών προβλημάτων με την ΑΔΠ.

Ζητήθηκε η γνώμη των ενδιαφερομένων φορέων σχετικά με τις διαφορετικές πτυχές της πρωτοβουλίας (ορισμός του προβλήματος και εναλλακτικές δυνατότητες για να αντιμετωπιστούν οι υφιστάμενες ελλείψεις) μέσα από:

- **Δημόσια διαδικτυακή διαβούλευση** σχετικά με «τη βελτίωση της ασφάλειας δικτύων και πληροφοριών στην ΕΕ», η οποία διήρκεσε από τις 23 Ιουλίου έως τις 15 Οκτωβρίου 2012. Συνολικά υποβλήθηκαν 169 απαντήσεις μέσω του ηλεκτρονικού εργαλείου, ενώ η Επιτροπή παράλαβε ακόμα 10 απαντήσεις γραπτώς.
- **Συζητήσεις με τα κράτη μέλη** στο πλαίσιο του ευρωπαϊκού φόρουμ των κρατών μελών (EFMS), διμερείς συναντήσεις καθώς και τη διάσκεψη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, η οποία διοργανώθηκε από την Επιτροπή και την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, στις 6 Ιουλίου 2012.
- Συζητήσεις με επιχειρήσεις του **ιδιωτικού τομέα** και με ενώσεις στο πλαίσιο της **ευρωπαϊκής** σύμπραξης **δημόσιου**-ιδιωτικού τομέα για την ανθεκτικότητα (EP3R), καθώς και σε διμερείς συναντήσεις.
- Συζητήσεις με τον **ENISA** και τη **CERT-EU**
- Συζητήσεις στο πλαίσιο της συνόδου του **2012 για το Ψηφιακό θεματολόγιο**

3. ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ

3.1. Καθορισμός του προβλήματος

Το πρόβλημα μπορεί να περιγραφεί ως συνολικά **ανεπαρκές επίπεδο προστασίας έναντι συμβάντων ασφάλειας που αφορούν δίκτυα και πληροφορίες, κινδύνους και απειλές σε ολόκληρη την ΕΕ, που επηρεάζουν την εύρυθμη λειτουργία της εσωτερικής αγοράς**.

Καθώς τα δίκτυα και τα συστήματα πληροφοριών είναι διασυνδεδεμένα και δεδομένου του παγκόσμιου χαρακτήρα του διαδικτύου, πολλά συμβάντα ΑΔΠ υπερβαίνουν τα εθνικά σύνορα και υπονομεύουν τη λειτουργία της εσωτερικής αγοράς.

Η παροχή διασυνοριακών υπηρεσιών μπορεί να καταστεί ανέφικτη, να ανασταλεί ή να διακοπεί λόγω παραβιάσεων ασφάλειας, όπως στην περίπτωση επιθέσεων που πλήττουν τους ιστοτόπους eBay και PayPal. Έχει υπογραμμιστεί η ανάγκη ταχείας ανάληψης δράσης για την αντιμετώπιση των προβλημάτων και την ανταλλαγή πληροφοριών σχετικά με σημαντικά συμβάντα στην περίπτωση επιθέσεων σε βάρος του Diginotar, της ολλανδικής εταιρείας έκδοσης διαδικτυακών πιστοποιητικών. Στον απόηχο παρελθόντων συμβάντων, τα κράτη μέλη αρχίζουν να θεσπίζουν τους δικούς τους κανονισμούς. Οι ασυντόνιστες κανονιστικές παρεμβάσεις μπορεί να οδηγήσουν σε κατακερματισμό και να υψώσουν φραγμούς στην εσωτερική αγορά, συνεπαγόμενες κόστος συμμόρφωσης για επιχειρήσεις που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη.

Το πρόβλημα αυτό αφορά όλες τις πτυχές της κοινωνίας και της οικονομίας (κυβερνήσεις, επιχειρήσεις και καταναλωτές). Ειδικότερα, ορισμένοι τομείς διαδραματίζουν ουσιαστικό ρόλο στην παροχή βασικών υπηρεσιών υποστήριξης για την οικονομία και την κοινωνία μας, ενώ η ασφάλεια των συστημάτων τους έχει ιδιαίτερη σημασία για τη λειτουργία της εσωτερικής αγοράς. **Οι τομείς αυτοί περιλαμβάνουν τις τράπεζες, τα χρηματιστήρια, την παραγωγή, τη μετάδοση και τη διανομή ενέργειας, τις μεταφορές (εναέριες, σιδηροδρομικές, θαλάσσιες), την υγεία, βασικές υπηρεσίες διαδικτύου και τη δημόσια διοίκηση. Από τη δημόσια διαβούλευση προέκυψε ισχυρή υποστήριξη από τους ενδιαφερομένους για την αντιμετώπιση θεμάτων ΑΔΠ στους τομείς αυτούς, καθώς και για την αντίστοιχη λήψη μέτρων σε επίπεδο ΕΕ.**

Η μη περαιτέρω λήψη μέτρων για την αντιμετώπιση του αυξανόμενου αριθμού των συμβάντων θα μπορούσε να αποτελέσει πλήγμα στην εμπιστοσύνη των καταναλωτών στις ηλεκτρονικές υπηρεσίες, κάτι το οποίο θα μπορούσε να υπονομεύσει την επίτευξη των στόχων του Ψηφιακού θεματολογίου.

3.2. Παράγοντες του προβλήματος

Το πρόβλημα που ορίζεται προκύπτει από μια σειρά παραγόντων.

Πρώτον, υπάρχει **άνισο επίπεδο ικανοτήτων σε εθνική κλίμακα σε ολόκληρη την ΕΕ**, γεγονός που δυσχεραίνει την οικοδόμηση εμπιστοσύνης μεταξύ ομολόγων, προϋπόθεση για τη συνεργασία και την ανταλλαγή πληροφοριών.

Δεύτερον, διαπιστώνεται **ανεπαρκής ανταλλαγή πληροφοριών σχετικά με συμβάντα, κινδύνους και απειλές**. Τα περισσότερα συμβάντα ΑΔΠ δεν δηλώνονται και περνούν απαρατήρητα, κυρίως λόγω της απροθυμίας των εταιρειών να γνωστοποιήσουν τις σχετικές πληροφορίες, διότι φοβούνται ότι θα θιγεί η φήμη τους ή ότι θα ζητηθούν ευθύνες. Η ανταλλαγή πληροφοριών στο πλαίσιο των υφιστάμενων εταιρικών σχέσεων / πλατφορμών δημόσιου-ιδιωτικού τομέα, όπως τα EFMS και EP3R περιορίζεται σε επίπεδο βέλτιστης πρακτικής.

4. ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΩΝ ΥΦΙΣΤΑΜΕΝΩΝ ΜΕΤΡΩΝ

4.1. Κενά στο υπάρχον κανονιστικό πλαίσιο

Οι ισχύοντες κανόνες δεν απαιτούν από οντότητες εκτός των εταιρειών τηλεπικοινωνιών να θεσπίσουν μέτρα διαχείρισης του κινδύνου NIS και να αναφέρουν συμβάντα ΑΔΠ . Ωστόσο, όλοι οι συμμετέχοντες φορείς που εξαρτώνται από συστήματα δικτύων και πληροφοριών αντιμετωπίζουν κινδύνους ασφάλειας. Τούτο συνεπάγεται άνισους όρους ανταγωνισμού, δεδομένου ότι το ίδιο συμβάν που επηρεάζει, για παράδειγμα, έναν φορέα παροχής τηλεπικοινωνιακών υπηρεσιών και μια εταιρεία παροχής φωνητικών υπηρεσιών μέσω υπηρεσιών IP πρέπει να κοινοποιείται στην αρμόδια εθνική αρχή στην πρώτη περίπτωση, όχι όμως στην τελευταία.

Όλοι οι συντελεστές που είναι υπεύθυνοι επεξεργασίας δεδομένων (π.χ. μια τράπεζα ή ένα νοσοκομείο) υποχρεούνται, βάσει του κανονιστικού πλαισίου για την προστασία των δεδομένων, να θεσπίσουν μέτρα ασφάλειας αναλογικά με τους κινδύνους που αντιμετωπίζουν. Αλλά οι υπεύθυνοι επεξεργασίας δεδομένων οφείλουν να κοινοποιήσουν μόνο τις παραβιάσεις της ασφάλειας όπου διακυβεύονται προσωπικά δεδομένα.

Η οδηγία 2008/114/ΕΚ του Συμβουλίου σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, καλύπτει μόνον τους τομείς της ενέργειας και των μεταφορών, ενώ μέχρι σήμερα λίγες μόνον ευρωπαϊκές υποδομές ζωτικής σημασίας έχουν αναγνωριστεί ως τέτοιες από τα κράτη μέλη. Η οδηγία δεν ορίζει υποχρέωση των φορέων να αναφέρουν σημαντικές παραβιάσεις της ασφάλειας και δεν θεσπίζει για τα κράτη μέλη μηχανισμούς συνεργασίας και αντίδρασης σε συμβάντα.

Οι συννομοθέτες εξετάζουν επί του παρόντος την πρόταση της Επιτροπής για έκδοση οδηγίας σχετικά με τις επιθέσεις κατά [1]συστημάτων πληροφοριών. Η παρούσα πρόταση καλύπτει μόνο την ποινικοποίηση συγκεκριμένων τύπων συμπεριφοράς, δεν εξετάζει όμως την πρόληψη κινδύνων και συμβάντων ΑΔΠ, την απόκριση σε συμβάντα ΑΔΠ και τον μετριασμό των επιπτώσεών τους.

4.2. Τα όρια της εθελοντικής προσέγγισης

Η εθελοντική προσέγγιση που ακολουθήθηκε έως τώρα είχε ως αποτέλεσμα άνισο επίπεδο ετοιμότητας και περιορισμένη συνεργασία.

Το EFMS έχει περιορισμένη αποστολή δεδομένου ότι τα κράτη μέλη δεν διαθέτουν πληροφορίες σχετικά με τα συμβάντα, τους κινδύνους και τις απειλές, ούτε συνεργάζονται για την αντιμετώπιση διασυνοριακών απειλών. Το EFMS δεν έχει εξουσία να απαιτήσει από τα μέλη του να διαθέτουν ορισμένες ελάχιστες δυνατότητες.

Ο ENISA δεν έχει επιχειρησιακές αρμοδιότητες και, για παράδειγμα, δεν μπορεί να παρέμβει για την επίλυση προβλημάτων της ΑΔΠ.

Η EP3R δεν διαθέτει επίσημο καθεστώς και δεν μπορεί να απαιτεί από τον ιδιωτικό τομέα την αναφορά συμβάντων στις εθνικές αρχές. Απουσιάζει στην EP3R ένα πλαίσιο για ασφαλή ανταλλαγή πληροφοριών και για διαβίβαση πληροφοριών σχετικά με απειλές, κινδύνους και συμβάντα για την ΑΔΠ.

5. ΑΝΑΓΚΗ ΠΑΡΕΜΒΑΣΗΣ ΤΗΣ ΕΕ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑΣ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑΣ

Η διασφάλιση της ΑΔΠ είναι ζωτικής σημασίας για την καλή λειτουργία της εσωτερικής αγοράς και για την ευημερία της κοινωνίας μας. Το άρθρο 114 της ΣΛΕΕ αποτελεί

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

κατάλληλη νομική βάση για εναρμόνιση των απαιτήσεων της ΑΔΠ και για την καθιέρωση κοινού ελάχιστου επιπέδου ασφάλειας σε όλη την ΕΕ.

Η παρέμβασης της Ένωσης στο πεδίο της ασφάλειας δικτύων και πληροφοριών αιτιολογείται βάσει της αρχής της **επικουρικότητας**, λόγω της διασυνοριακής φύσης του προβλήματος και της αυξημένης αποτελεσματικότητας (και, συνεπώς, της προστιθέμενης αξίας) των υφιστάμενων εθνικών πολιτικών που θα προέκυπταν από τη δράση σε επίπεδο ΕΕ.

Για να εξασφαλιστεί συνεργασία που θα περιλαμβάνει όλα τα κράτη μέλη, είναι απαραίτητο να βεβαιωθεί ότι όλα διαθέτουν το απαιτούμενο ελάχιστο επίπεδο δυνατοτήτων. Επιπλέον, είναι σαφές ότι, συντονισμένες και συνεργατικές πολιτικές ενέργειες για την ασφάλεια δικτύων και πληροφοριών μπορούν να έχουν ισχυρή ευεργετική επίδραση στην ουσιαστική προστασία των θεμελιωδών δικαιωμάτων και, ειδικότερα, στο δικαίωμα της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής.

Τα μέτρα στο πλαίσιο της προτιμώμενης επιλογής είναι δικαιολογημένα για λόγους **αναλογικότητας**, δεδομένου ότι οι απαιτήσεις για τα κράτη μέλη έχουν καθοριστεί στο ελάχιστο αναγκαίο επίπεδο για την επίτευξη επαρκούς ετοιμότητας και για να καταστεί δυνατή η συνεργασία που θα βασίζεται στην εμπιστοσύνη, ενώ οι απαιτήσεις, για επιχειρήσεις και δημόσιες αρχές, να προβλέπουν τη διαχείριση κινδύνου και να αναφέρουν συμβάντα ισχύουν αποκλειστικά για στόχους ζωτικής σημασίας και συνεπάγονται μέτρα αναλογικά προς τους κινδύνους, που αφορούν συμβάντα με σημαντικό αντίκτυπο. Επιπλέον, τα μέτρα στο πλαίσιο της προτιμώμενης επιλογής δεν συνεπάγονται δυσανάλογες δαπάνες.

6. ΣΤΟΧΟΙ

Ο γενικός στόχος είναι να αυξηθεί το επίπεδο προστασίας έναντι των συμβάντων, κινδύνων και απειλών που αφορούν την ασφάλεια δικτύων και πληροφοριών σε όλη την ΕΕ. Οι ειδικοί στόχοι είναι οι εξής:

- **Στόχος 1** - να θεσπιστεί στα κράτη μέλη ελάχιστο κοινό επίπεδο ΑΔΠ και, συνεπώς, να αυξηθεί το συνολικό επίπεδο ετοιμότητας και απόκρισης.
- **Στόχος 2** - Να βελτιωθεί η συνεργασία για την ασφάλεια δικτύων και πληροφοριών σε επίπεδο ΕΕ με σκοπό την αποτελεσματική πάταξη διασυνοριακών συμβάντων και απειλών.
- **Στόχος 3** - Να διαμορφωθεί κλίμα διαχείρισης κινδύνου και να βελτιωθεί η ανταλλαγή πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα.

7. ΕΠΙΛΟΓΕΣ ΠΟΛΙΤΙΚΗΣ

Οι επιλογές πολιτικής που εξετάστηκαν στην παρούσα εκτίμηση του αντικτύπου είναι: Συνέχιση της σημερινής κατάστασης, κανονιστική και μικτή προσέγγιση. Απορρίφθηκε η πιθανή επιλογή που συνίσταται σε παύση όλων των δραστηριοτήτων της ΕΕ σχετικά με την ΑΔΠ.

7.1. Επιλογή 1 – Διατήρηση της υφιστάμενης κατάστασης («βασικό σενάριο)

Η Επιτροπή, με τη συνδρομή του ENISA, θα εξακολουθήσει να εφαρμόζει την τρέχουσα εθελοντική προσέγγιση καλώντας τα κράτη μέλη να συστήσουν σε εθνικό επίπεδο ικανότητες ΑΔΠ (π.χ. ομάδες CERT, εθνικά σχέδια έκτακτης ανάγκης/συμβάντων στον κυβερνοχώρο, εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο) και να συνεργάζονται σε επίπεδο ΕΕ (π.χ. μέσω δικτύου CERT στην Ευρώπη και μέσω ενός ευρωπαϊκού σχεδίου έκτακτης ανάγκης/συνεργασίας για συμβάντα στον κυβερνοχώρο).

7.2. Επιλογή 2 - Κανονιστική προσέγγιση

Η Επιτροπή θα απαιτούσε από όλα τα κράτη μέλη να συγκροτήσουν τουλάχιστον ένα ελάχιστο επίπεδο των εθνικών δυνατοτήτων (ομάδες CERT, αρμόδιες αρχές, εθνικά σχέδια συμβάντων / έκτακτης ανάγκης στον κυβερνοχώρο, εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο).

Βάσει της κανονιστικής αυτής επιλογής, οι αρμόδιες εθνικές αρχές και οι ομάδες CERT θα αποτελούσαν μέρος ενός **δικτύου** συνεργασίας σε ενωσιακό επίπεδο. Στο πλαίσιο του δικτύου, οι αρχές και οι ομάδες CERT θα ανταλλάσσουν πληροφορίες και θα συνεργάζονται για την αντιμετώπιση απειλών και συμβάντων σχετικά με την ΑΔΠ σύμφωνα με το **ευρωπαϊκό σχέδιο έκτακτης ανάγκης / συνεργασίας για συμβάντα στον κυβερνοχώρο** επί του οποίου πρέπει να συμφωνήσουν τα κράτη μέλη.

Εταιρείες (εκτός των πολύ μικρών επιχειρήσεων) σε ορισμένους κρίσιμους τομείς, δηλ. στις τράπεζες, την ενέργεια (ηλεκτρική ενέργεια και φυσικό αέριο), τις μεταφορές, την υγεία, τους παρόχους βασικών υπηρεσιών διαδικτύου και τη δημόσια διοίκηση, θα κληθούν να αξιολογήσουν τους κινδύνους που αντιμετωπίζουν και να θεσπίσουν κατάλληλα και αναλογικά μέτρα για την επιμέτρηση των πραγματικών κινδύνων. Επιπλέον, οι εν λόγω φορείς θα πρέπει να αναφέρουν στις αρμόδιες αρχές τα συμβάντα που θέτουν σοβαρά σε κίνδυνο τη λειτουργία των οικείων δικτύων και συστημάτων πληροφοριών, με σημαντικό, επομένως, αντίκτυπο στη συνέχεια παροχής των υπηρεσιών και του εφοδιασμού σε προϊόντα που εξαρτώνται από τα συστήματα δικτύων και πληροφοριών. Το καθεστώς αυτό ακολουθεί εκείνο του άρθρου 13 α & β της οδηγίας πλαίσιο για τις ηλεκτρονικές επικοινωνίες.

7.3. Επιλογή 3 - Μικτή προσέγγιση

Η Επιτροπή θα συνδύαζε εθελοντικές πρωτοβουλίες με βάση την προθυμία των κρατών μελών, με στόχο τη συγκρότηση ή ενίσχυση των ικανοτήτων των κρατών μελών στο πεδίο της ασφάλειας δικτύων και πληροφοριών και την καθιέρωση μηχανισμών συνεργασίας σε ενωσιακό επίπεδο, με κανονιστικές απαιτήσεις για τους κύριους ιδιωτικούς φορείς και τη δημόσια διοίκηση.

Οι εθελοντικές πρωτοβουλίες θα ήταν κατ' ουσίαν παρεμφερείς με όσες έχουν αναληφθεί στο πλαίσιο της επιλογής 1, ενώ οι κανονιστικές απαιτήσεις θα ήταν ταυτόσημες με όσες έχουν επιβληθεί στο πλαίσιο της επιλογής 2, όσον αφορά τόσο τις στοχευόμενες οντότητες όσο και την ουσία των υποχρεώσεων.

Ο ENISA θα παρείχε στην Επιτροπή, στα κράτη μέλη και στον ιδιωτικό τομέα υποστήριξη και τεχνική εμπειρογνωμοσύνη, π.χ. με έκδοση τεχνικών κατευθυντήριων γραμμών και συστάσεων.

8. ΑΝΑΛΥΣΗ ΤΟΥ ΑΝΤΙΚΤΥΠΟΥ

Εκτός από το επίπεδο της ασφάλειας, η αξιολόγηση καλύπτει τον οικονομικό και κοινωνικό αντίκτυπο των τριών επιλογών. Καλύπτει επίσης το κόστος που συνεπάγονται οι επιλογές πολιτικής 2 και 3.

Καμία από τις εν λόγω εναλλακτικές λύσεις δεν θα έχει αντίκτυπο στο περιβάλλον, ο οποίος να μπορεί να προβλεφθεί με ακρίβεια.

8.1. Επιλογή 1 – Διατήρηση της υφιστάμενης κατάστασης («βασικό σενάριο)

Επίπεδο ασφάλειας: Είναι απίθανο όλα τα κράτη μέλη να επιτύχουν συγκρίσιμα εθνικά επίπεδα ικανοτήτων και ετοιμότητας που είναι απαραίτητα ώστε να βελτιώσουν την ασφάλεια και να καταστήσουν δυνατή τη συνεργασία και την ανταλλαγή εμπιστευμένων

πληροφοριών σε ενωσιακό επίπεδο. Σε ό,τι αφορά τη διαχείριση κινδύνων και την αυξημένη διαφάνεια σχετικά με συμβάντα δεν θα επιτευχθούν ίσοι όροι ανταγωνισμού, επομένως θα εξακολουθήσουν να ισχύουν ρυθμιστικά κενά.

Οικονομικός αντίκτυπος: Ο αντίκτυπος θα εξαρτηθεί από το βαθμό στον οποίο τα κράτη μέλη θα ακολουθήσουν τις συστάσεις της Επιτροπής. Το ανεπαρκές επίπεδο ασφάλειας στα λιγότερο ανεπτυγμένα κράτη μέλη θα υπονόμευε τα επίπεδα ανταγωνιστικότητας και ανάπτυξής τους και θα εξέθετε σε κινδύνους και συμβάντα. Λαμβάνοντας υπόψη τις τρέχουσες τάσεις, τα συμβάντα ΑΔΠ θα καθίστανται ολοένα και πιο ορατά για τις επιχειρήσεις και τους καταναλωτές και θα παρεμποδίζουν την ολοκλήρωση της εσωτερικής αγοράς.

Κοινωνικός αντίκτυπος: Η συνέχιση και η αναμενόμενη επιδείνωση των συμβάντων, κινδύνων και απειλών θα επηρέαζαν αρνητικά την επιγραμμική (διαδικτυακή) εμπιστοσύνη των πολιτών.

8.2. Επιλογή 2 - Κανονιστική προσέγγιση

Επίπεδο ασφάλειας: Οι υποχρεώσεις που επιβάλλονται στα κράτη μέλη θα διασφάλιζαν ότι όλα τους είναι επαρκώς εξοπλισμένα και ότι θα συμβάλουν στη δημιουργία κλίματος αμοιβαίας εμπιστοσύνης, προϋπόθεση για αποτελεσματική συνεργασία σε ενωσιακό επίπεδο.

Η εισαγωγή απαιτήσεων για εφαρμογή διαχείρισης κινδύνων ΑΔΠ στη δημόσια διοίκηση και στους κύριους ιδιωτικούς συντελεστές θα αποτελούσε σημαντικό κίνητρο για την αποτελεσματική διαχείριση και επιμέτρηση των κινδύνων ασφάλειας. Οι συνολικές συμπληρωματικές δαπάνες που θα επιβάρυναν όλους τους τομείς στην ΕΕ για την κάλυψη αυτών των απαιτήσεων θα κυμαίνονταν από **1 έως 2 δισεκατ. ευρώ**. Το ειδικό *κόστος συμμόρφωσης* ***ανά μικρή και μεσαία επιχείρηση*** *θα είναι της τάξης των* ***2500 και 5000 ευρώ***.

Οικονομικός αντίκτυπος: Ως αποτέλεσμα του αυξημένου επιπέδου ασφάλειας, θα μειώνονταν οι οικονομικές ζημίες που συνδέονται με κινδύνους και συμβάντα ΑΔΠ. Η εμπιστοσύνη επιχειρήσεων και καταναλωτών στον ψηφιακό κόσμο θα ενισχυόταν προς όφελος της εσωτερικής αγοράς. Η προώθηση ενισχυμένης αντίληψης ως προς τη διαχείριση κινδύνων θα τόνωνε τη ζήτηση για ασφαλή προϊόντα και λύσεις ΤΠΕ.

Κοινωνικός αντίκτυπος: Η επίτευξη υψηλότερου επιπέδου ασφάλειας θα βελτίωνε την επιγραμμική εμπιστοσύνη των πολιτών που θα μπορούσαν να αποκομίσουν όλα τα οφέλη από τον ψηφιακό κόσμο (π.χ. μέσα κοινωνικής δικτύωσης, ηλε-μάθηση, ηλ-υγεία).

8.3. Επιλογή 3 - Μικτή προσέγγιση

Επίπεδο ασφάλειας: Όπως στην επιλογή 1, δεν υπάρχει εγγύηση ότι το επίπεδο ασφάλειας βάσει των εθνικών ικανοτήτων NIS και η συνεργασία σε ενωσιακό επίπεδο θα βελτιώνονταν, ως αποτέλεσμα εθελοντικών πρωτοβουλιών. Η θέσπιση απαιτήσεων ασφάλειας για τη δημόσια διοίκηση και τους κύριους ιδιωτικούς συντελεστές, αφετέρου, θα δημιουργούσε ισχυρό κίνητρο για τη διαχείριση και την επιμέτρηση των κινδύνων για την ασφάλεια. Οι εν λόγω μηχανισμοί θα ήταν, ωστόσο, αναποτελεσματικοί στα κράτη μέλη που δεν θα ακολουθούσαν τις συστάσεις της Επιτροπής για τη συγκρότηση ικανοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

Οικονομικός αντίκτυπος: Ο ρυθμός ανάπτυξης θα διέφερε σημαντικά μεταξύ των κρατών μελών. Το ανεπαρκές επίπεδο ασφάλειας στα λιγότερο αναπτυγμένα κράτη μέλη θα υπονόμευε τα επίπεδα ανταγωνιστικότητας και ανάπτυξής τους και θα τα εξέθετε στις επιπτώσεις κινδύνων και συμβάντων.

Κοινωνικός αντίκτυπος: Η συνέχιση και η αναμενόμενη επιδείνωση των συμβάντων, κινδύνων και απειλών θα επηρέαζαν αρνητικά τη διαδικτυακή εμπιστοσύνη, ειδικά στα κράτη μέλη που δεν αντιμετωπίζουν την ΑΔΠ ως προτεραιότητα.

9. ΣΥΓΚΡΙΣΗ ΤΩΝ ΕΠΙΛΟΓΩΝ

Η επιλογή 1 και 3 δεν θεωρούνται ζωτικές για την επίτευξη των στόχων πολιτικής και, ως εκ τούτου, δεν συνιστώνται, δεδομένου ότι η αποτελεσματικότητά τους θα εξαρτηθεί από το κατά πόσον η εθελοντική προσέγγιση θα είναι πράγματι σε θέση να επιτύχει ένα ελάχιστο επίπεδο ασφάλειας δικτύων και πληροφοριών, ενώ, όσον αφορά την επιλογή 3, θα εξαρτηθεί από την προθυμία των κρατών μελών να συγκροτήσουν ικανότητες και να συνεργαστούν σε διασυνοριακό επίπεδο.

Η επιλογή 2 είναι η προτιμότερη, δεδομένου ότι στο πλαίσιο της επιλογής αυτής, η προστασία των καταναλωτών, των επιχειρήσεων και των κυβερνήσεων της ΕΕ έναντι συμβάντων, απειλών και κινδύνων ΑΔΠ αναμένεται να βελτιωθεί σημαντικά. Επιπλέον, βάζοντας τάξη στα του οίκου της, η ΕΕ θα είναι σε θέση να επεκτείνει τη διεθνή της εμβέλεια και να ενισχυθεί περαιτέρω η αξιοπιστία της ως εταίρου για συνεργασία σε διμερές και πολυμερές επίπεδο. Ως εκ τούτου, η ΕΕ θα βρεθεί επίσης σε καλύτερη θέση για να προωθήσει τα θεμελιώδη δικαιώματα και τις θεμελιώδεις αξίες της ΕΕ στο εξωτερικό.

10. ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ

Στο κεφάλαιο 10 της έκθεσης εκτίμησης του αντίκτυπου περιγράφεται σειρά βασικών δεικτών της προόδου προς την επίτευξη των στόχων. Οι δείκτες αυτοί περιλαμβάνουν, για παράδειγμα:

- Για τον στόχο 1, τον αριθμό των κρατών μελών που έχουν ορίσει αρμόδια αρχή ΑΔΠ και ομάδα CERT ή που έχουν θεσπίσει εθνική στρατηγική ασφάλειας στον κυβερνοχώρο και εθνικό σχέδιο έκτακτης ανάγκης / συνεργασίας για συμβάντα στον κυβερνοχώρο.
- Για τον στόχο 2, τον αριθμό των αρμόδιων αρχών των κρατών μελών και των ομάδων CERT που συμμετέχουν στο δίκτυο και τον όγκο των πληροφοριών που ανταλλάσσονται στο πλαίσιο του δικτύου σχετικά με κινδύνους και συμβάντα ΑΔΠ για τον στόχο 3, το επίπεδο των επενδύσεων στην ασφάλεια δικτύων και πληροφοριών εκ μέρους κύριων ιδιωτικών συντελεστών και της δημόσιας διοίκησης, καθώς και τον αριθμό των κοινοποιήσεων συμβάντων ΑΔΠ που είχαν σημαντικό αντίκτυπο.