



ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 13.9.2017
SWD(2017) 501 final

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

ΠΕΡΙΛΗΨΗ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ

που συνοδεύει το έγγραφο

Πρόταση για ΚΑΝΟΝΙΣΜΟ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ

**σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο»,
και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την
πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας
πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»)**

{ COM(2017) 477 final }

{ SWD(2017) 500 final }

{ SWD(2017) 502 final }

A. ΥΠΑΡΧΕΙ ΑΝΑΓΚΗ ΓΙΑ ΑΝΑΛΗΨΗ ΔΡΑΣΗΣ

Ποιο είναι το πρόβλημα και γιατί συνιστά πρόβλημα;

Οι ψηφιακές τεχνολογίες και το διαδίκτυο είναι η ραχοκοκαλιά της οικονομίας και της κοινωνίας στην ΕΕ. Νευραλγικοί οικονομικοί τομείς, όπως οι μεταφορές, η ενέργεια, η υγεία ή ο χρηματοπιστωτικός τομέας έχουν καταστεί ολοένα περισσότερο εξαρτημένοι από συστήματα δικτύων και πληροφοριών για την εκτέλεση του κύριου μέρους των δραστηριοτήτων τους. Το διαδίκτυο των πραγμάτων συνδέει αντικείμενα και πρόσωπα μέσω δικτύων επικοινωνίας. Η νέα αυτή πραγματικότητα δημιουργεί πρωτοφανείς ευκαιρίες, ταυτόχρονα όμως και τρωτά σημεία. Πράγματι, τα συμβάντα στον κυβερνοχώρο παρουσιάζουν δυναμική ανάπτυξη. Η πολυπλοκότητά τους, η συχνότητα και η «έκταση» του αντίκτυπού τους — από την πρόσβαση σε βασικές υπηρεσίες έως τις δημοκρατικές διαδικασίες — πρόκειται να αυξηθούν ακόμη περισσότερο.

Στο πλαίσιο αυτό, έχουν αναγνωριστεί τα ακόλουθα αλληλένδετα προβλήματα:

- Κατακερματισμός πολιτικών και προσεγγίσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο, μεταξύ των κρατών μελών.
- Διασπορά πόρων και μεθοδολογικών προσεγγίσεων της ασφάλειας στον κυβερνοχώρο μεταξύ θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ.
- Ανεπαρκής ευαισθητοποίηση πολιτών και επιχειρήσεων ως προς τις απειλές στον κυβερνοχώρο και ανεπαρκής πληροφόρηση όσον αφορά τα χαρακτηριστικά ασφάλειας των προϊόντων και υπηρεσιών ΤΠΕ που αγοράζουν, σε συνδυασμό με την αυξανόμενη παρουσία πολλαπλών, εθνικών και κλαδικών, συστημάτων πιστοποίησης.

Αυτά τα προβλήματα επιδρούν στη συνολική ανθεκτικότητα του κυβερνοχώρου της ΕΕ και στην αποτελεσματική λειτουργία της εσωτερικής αγοράς.

Τι πρέπει να επιτευχθεί;

Οι ειδικοί στόχοι πολιτικής της εν λόγω πρωτοβουλίας είναι οι ακόλουθοι:

1. Αύξηση των ικανοτήτων και της ετοιμότητας των κρατών μελών και των επιχειρήσεων, ιδίως όσον αφορά υποδομές ζωτικής σημασίας.
2. Βελτίωση της συνεργασίας και του συντονισμού μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ.
3. Αύξηση των ικανοτήτων σε επίπεδο ΕΕ προς συμπλήρωση της δράσης των κρατών μελών, ιδίως όσον αφορά κρίσεις στον κυβερνοχώρο με διασυνοριακή διάσταση.
4. Αύξηση της ευαισθητοποίησης πολιτών και επιχειρήσεων σχετικά με τα θέματα ασφάλειας του κυβερνοχώρου.
5. Αύξηση της συνολικής διαφάνειας σε θέματα διασφάλισης της κυβερνοασφάλειας προϊόντων και υπηρεσιών ΤΠΕ, για την ενίσχυση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά και στην ψηφιακή καινοτομία.
6. Αποτροπή κατακερματισμού των καθεστώτων πιστοποίησης στην ΕΕ, καθώς και των σχετικών απαιτήσεων ασφάλειας και κριτηρίων αξιολόγησης στα διάφορα κράτη μέλη και

τομείς.

Ποια είναι η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ;

Δεδομένου ότι η ψηφιοποίηση και η διασύνδεση οικονομίας και κοινωνίας έχουν παγκόσμια εμβέλεια, το μέγεθος των προβλημάτων υπερβαίνει κατά πολύ την επικράτεια του μεμονωμένου κράτους μέλους. Απαιτείται, κατά συνέπεια, παρέμβαση σε ενωσιακό επίπεδο. Στο σημερινό πλαίσιο και εξετάζοντας τα μελλοντικά σενάρια, φαίνεται ότι οι μεμονωμένες δράσεις από τα κράτη μέλη και μια κατακερματισμένη προσέγγιση της ασφάλειας στον κυβερνοχώρο, ιδίως της ισχυρής διασυνοριακής διάστασής της, δεν συμβάλλουν σε αύξηση της συλλογικής ενωσιακής ανθεκτικότητας στον κυβερνοχώρο.

B. ΛΥΣΕΙΣ

Ποιες είναι οι επιλογές για την επίτευξη των στόχων; Υπάρχει προτιμώμενη επιλογή ή όχι;

Η παρούσα εκτίμηση επιπτώσεων εξετάζει μια συγκεκριμένη δέσμη πολιτικών επιλογών, που καλύπτει την επανεξέταση του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την πιστοποίηση της ασφάλειας ΤΠΕ.

Επανεξέταση του ENISA

Επιλογή 0 — **Βασικό σενάριο** — Η επιλογή αυτή συνεπάγεται διατήρηση του status quo. Η εντολή του ENISA θα διευρυνθεί ενώ στόχοι και καθήκοντα του Οργανισμού θα παραμείνουν ως επί το πλείστον αμετάβλητοι, λαμβάνοντας παράλληλα υπόψη τα καθήκοντα που έχουν ανατεθεί στον ENISA από μεταγενέστερη ενωσιακή νομοθεσία (π.χ. την οδηγία για την ασφάλεια δικτύων και πληροφοριών).

Επιλογή 1 — **Λήξη εντολής του ENISA** (παύση ENISA). Η επιλογή αυτή θα οδηγούσε στη παύση του ENISA μετά το πέρας της εντολής του (τον Ιούνιο του 2020), και ενδεχομένως σε ανακατανομή των αρμοδιοτήτων/δραστηριοτήτων σε ενωσιακό ή/και εθνικό επίπεδο.

Επιλογή 2 — **«Αναμορφωμένος ENISA»**. Η επιλογή αυτή βασίζεται στην υφιστάμενη εντολή του ENISA αποβλέποντας σε υιοθέτηση επιλεκτικών τροποποιήσεων που λαμβάνουν υπόψη την εξέλιξη του πλαισίου της ασφάλειας στον κυβερνοχώρο. Ο Οργανισμός θα αποκτήσει μόνιμη εντολή, με βάση τα ακόλουθα βασικά δομοστοιχεία: στήριξη στην εκπόνηση και εφαρμογή ενωσιακής πολιτικής· δημιουργία ικανοτήτων· γνώση και πληροφόρηση· καθήκοντα συναφή με την αγορά· έρευνα και καινοτομία· καθώς και επιχειρησιακή συνεργασία και διαχείριση κρίσεων.

Επιλογή 3 — **Οργανισμός της ΕΕ για την ασφάλεια στον κυβερνοχώρο με πλήρη επιχειρησιακή ικανότητα**. Η επιλογή αυτή συνεπάγεται αναμόρφωση του ENISA, συνενώνοντας τρεις βασικές λειτουργίες: 1. Πολιτική/συμβουλευτική λειτουργία· 2. Κέντρο πληροφόρησης και εμπειρογνωμοσύνης, και 3. Ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) Σε μεγάλο βαθμό, η επιλογή αυτή συνεπάγεται την ίδια αλλαγή του πεδίου εφαρμογής της εντολής όπως στην επιλογή 2. Ωστόσο, θα προστεθούν επιπλέον καθήκοντα στο πεδίο της αντίδρασης σε συγκεκριμένα συμβάντα και της διαχείρισης κρίσεων, ώστε ο οργανισμός να καλύπτει το σύνολο του κύκλου ζωής της ασφάλειας στον

κυβερνοχώρο, διαλαμβάνοντας την αποτροπή, την ανίχνευση και την αντιμετώπιση συμβάντων στον κυβερνοχώρο.

Πιστοποίηση

Επιλογή 0 - Βασικό σενάριο — «Απραξία». Στο πλαίσιο αυτής της επιλογής, η Επιτροπή διατηρεί το υφιστάμενο καθεστώς και δεν αναλαμβάνει καμία πολιτική ή νομοθετική δράση.

Επιλογή 1 - Μη νομοθετικά μέτρα (μη δεσμευτικό δίκαιο). Στο πλαίσιο αυτής της επιλογής, η Επιτροπή χρησιμοποιεί ήπια μέσα πολιτικής (π.χ. ερμηνευτικές ανακοινώσεις, στήριξη των πρωτοβουλιών αυτορύθμισης σε ενωσιακό επίπεδο και δραστηριότητες τυποποίησης) με σκοπό τη βελτίωση της διαφάνειας και τη μείωση της αποσπασματικότητας.

Επιλογή 2 - Ενωσιακή νομοθετική πράξη για την επέκταση της συμφωνίας SOG-IS σε όλα τα κράτη μέλη. Στο πλαίσιο της εν λόγω επιλογής πολιτικής, η Επιτροπή προτείνει νομοθετική πράξη με την οποία η ιδιότητα του μέλους επεκτείνεται νομικώς σε όλα τα κράτη μέλη.

Επιλογή 3 - Γενικό πλαίσιο πιστοποίησης της ασφάλειας των ΤΠΕ. Η επιλογή αυτή συνεπάγεται τη θέσπιση ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας των ΤΠΕ (συμπεριλαμβανομένης ομάδας εμπειρογνομόνων αποτελούμενης από εθνικές αρχές) κατά το δυνατόν με βάση υφιστάμενα συστήματα πιστοποίησης της ασφάλειας ΤΠΕ. Κατ' ουσίαν, το πλαίσιο καθιστά δυνατή την καθιέρωση συστημάτων πιστοποίησης που θα γίνουν δεκτά σε όλα τα κράτη μέλη.

Η προτιμώμενη επιλογή είναι συνδυασμός της επιλογής 2 για τον ENISA και της επιλογής 3 για την πιστοποίηση.

Ποια είναι τα διάφορα ενδιαφερόμενα μέρη; Ποιος υποστηρίζει ποιάν επιλογή;

Η συντριπτική πλειοψηφία των ενδιαφερομένων όλων των κατηγοριών (κράτη μέλη, κλάδος, ερευνητική κοινότητα, θεσμικά όργανα της ΕΕ) που έλαβαν μέρος στις διαβουλεύσεις φαίνεται να συμφωνεί με την προτιμώμενη επιλογή, καθώς ευνοείται η ενίσχυση του ENISA και η δημιουργία ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας των ΤΠΕ.

Ειδικότερα, υπάρχει συναίνεση για την ανάγκη (ως ελάχιστο) ενός εύρυθμα λειτουργούντος οργανισμού της ΕΕ που διαθέτει μόνιμη εντολή, τους απαραίτητους πόρους και είναι εντεταλμένος να αντιμετωπίσει τις σημερινές και τις μελλοντικές προκλήσεις για την ασφάλεια στον κυβερνοχώρο. Υπάρχει επίσης ευρεία συμφωνία μεταξύ των ενδιαφερομένων για τη δημιουργία εθελοντικού ευρωπαϊκού πλαισίου, με δυνατότητα κλιμάκωσης.

Από την πλευρά του κλάδου, η λύση αυτή για πιστοποίηση υποστηρίζεται από επιχειρήσεις που ήδη υπόκεινται σε απαιτήσεις πιστοποίησης και οι οποίες θα μπορούσαν να ωφεληθούν από ένα σύστημα ενωσιακής κλίμακας που θα βασίζεται σε αμοιβαία αναγνώριση πιστοποιητικών στα κράτη μέλη. Η άποψη αυτή υποστηρίζεται επίσης από τις ΜΜΕ, οι οποίες επιβαρύνονται περισσότερο αν ήδη πρέπει ή αν υποχρεωθούν να συμμετέχουν σε διαφορετικές μεταξύ τους διαδικασίες πιστοποίησης στα κράτη μέλη. Ορισμένα κράτη μέλη, ιδίως εκείνα με περιορισμένους πόρους, καθώς και ορισμένοι εκπρόσωποι του κλάδου και των θεσμικών οργάνων της ΕΕ εξέφρασαν επίσης θετικές απόψεις όσον αφορά την επιλογή 3 για τον ENISA.

C. ΑΝΤΙΚΤΥΠΟΣ ΤΗΣ ΠΡΟΤΙΜΩΜΕΝΗΣ ΕΠΙΛΟΓΗΣ

Ποια είναι τα οφέλη της προτιμώμενης επιλογής (αν υπάρχουν, αλλιώς των κυριότερων επιλογών);

Σύμφωνα με την προτιμώμενη επιλογή, η ΕΕ θα διαθέτει έναν οργανισμό, εστιασμένο στην υποστήριξη των κρατών μελών, των θεσμικών οργάνων της ΕΕ και των επιχειρήσεων σε πεδία όπου θα μπορούσε να προκύψει η μεγαλύτερη προστιθέμενη αξία. Πρόκειται για: στήριξη της εφαρμογής της οδηγίας για την ασφάλεια δικτύων και πληροφοριών· εκπόνηση και εφαρμογή πολιτικής· γνώση και επίγνωση των πληροφοριών· έρευνα· επιχειρησιακή συνεργασία και κρίση· αγορά. Ειδικότερα, ο ENISA θα στηρίζει την πολιτική της ΕΕ στο πεδίο της πιστοποίησης της ασφάλειας ΤΠΕ, εξασφαλίζοντας διοικητική συνέχεια και τεχνική διαχείριση ενός ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας ΤΠΕ. Ένα τέτοιο πλαίσιο θα θεσπίσει αποτελεσματικά ένα σύνολο κανόνων σχετικά με τη διαχείριση της πιστοποίησης της ασφάλειας ΤΠΕ στην ΕΕ, γεγονός που θα προωθήσει ένα σύστημα αμοιβαίας αναγνώρισης των πιστοποιητικών που εκδίδονται στα κράτη μέλη. Η λύση που συνδυάζει τις επιλογές αυτές θεωρείται η αποτελεσματικότερη ώστε η ΕΕ να επιτύχει τους καθορισμένους στόχους της: αύξηση των ικανοτήτων της ασφάλειας στον κυβερνοχώρο· ετοιμότητα· συνεργασία· ευαισθητοποίηση· διαφάνεια· και αποτροπή κατακερματισμού της αγοράς. Η επιλογή αυτή παρουσιάζει επίσης τη μεγαλύτερη συνοχή με τις προτεραιότητες πολιτικής, δεδομένου ότι εντάσσεται στη στρατηγική για την ασφάλεια στον κυβερνοχώρο και τις συναφείς πολιτικές (π.χ. την οδηγία για την ασφάλεια δικτύων και πληροφοριών), καθώς και την στρατηγική για την ψηφιακή ενιαία αγορά. Επιπλέον, η επιλογή αυτή θα επιτύχει τους στόχους μέσω εύλογης χρήσης των πόρων.

Ποιο είναι το κόστος της προτιμώμενης επιλογής (αν υπάρχει, αλλιώς των κυριότερων επιλογών);

Παρά την απόκτηση νέων ρόλων, ο αναμορφωμένος «ENISA» θα παρέμενε ευέλικτη οργάνωση. Η απαιτούμενη οικονομική συνεισφορά από τον προϋπολογισμό της ΕΕ θα είναι υψηλότερη από ό,τι σήμερα, αλλά θα παρέμενε αρκετά χαμηλότερη από των άλλων οργανισμών που λειτουργούν σε κρίσιμα πεδία.

Η δημιουργία ευρωπαϊκού πλαισίου πιστοποίησης της ασφάλειας ΤΠΕ δεν θα επιφέρει πρόσθετο αρχικό κόστος στον κλάδο (συμπεριλαμβανομένων των ΜΜΕ). Αντιθέτως, θα οδηγήσει σε σημαντική εξοικονόμηση για τις επιχειρήσεις που ήδη πιστοποιούν τα προϊόντα τους ή είναι πρόθυμες να διεξαγάγουν πιστοποίηση ασφάλειας, με ευνοϊκές συνέπειες για την ανταγωνιστικότητά τους σε παγκόσμιο επίπεδο. Από την άλλη πλευρά, αυτό θα συνεπαγόταν ορισμένες δημοσιονομικές αναλήψεις υποχρεώσεων ώστε να εξασφαλιστεί η διατήρηση του πλαισίου, το οποίο θα αναλάμβανε κυρίως ο αναμορφωμένος «ENISA», όσον αφορά τεχνικά και γραμματειακά καθήκοντα.

Θα υπάρξει σημαντικός αντίκτυπος στους εθνικούς προϋπολογισμούς και στις εθνικές διοικήσεις;

Όχι. Το κόστος για την ενίσχυση του ENISA θα καλυφθεί κυρίως από τον προϋπολογισμό της ΕΕ, ενώ τα κράτη μέλη θα εξακολουθήσουν να είναι σε θέση να παρέχουν εθελοντικές οικονομικές συνεισφορές στον Οργανισμό. Όσο για την πιστοποίηση, ο κύριος αντίκτυπος στους εθνικούς προϋπολογισμούς και τις διοικήσεις θα προκύψει από την, κατά περίπτωση, σύσταση της αρχής πιστοποίησης.

Θα υπάρξουν άλλες σημαντικές επιπτώσεις;

Όχι.

Και η αναλογικότητα;

Η προτιμώμενη επιλογή περιλαμβάνει ισορροπημένα μέτρα, που κρίνονται ανεξαιρέτως απαραίτητα για την επίτευξη των διακυβευόμενων στόχων χωρίς να επιβαρύνουν υπέρμετρα τους σχετικούς ενδιαφερόμενους φορείς. Υπό το πρίσμα αυτό, η εν λόγω πρωτοβουλία θεωρείται σύμφωνη με την αρχή της αναλογικότητας.

D. ΕΠΑΚΟΛΟΥΘΕΣ ΕΝΕΡΓΕΙΕΣ

Πότε θα επανεξεταστεί η πολιτική;

Η πρώτη αξιολόγηση προτείνεται πλέον να πραγματοποιηθεί πέντε έτη από την έναρξη ισχύος του νομικού μέσου. Η Επιτροπή θα υποβάλει ακολούθως έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο σχετικά με την αξιολόγησή της, συνοδευόμενη, εφόσον ενδείκνυται, από πρόταση επανεξέτασής του. Περαιτέρω αξιολογήσεις θα διενεργούνται ανά πενταετία.