Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 29 Μαρτίου 2022
(OR. en)

Διοργανικός φάκελος:
2022/0084(COD)

7670/22
ADD 7

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	22 Μαρτίου 2022
Αποδέκτης:	κ. Jeppe TRANHOLM-MIKKELSEN, Γενικός Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	SWD(2022) 65 final
Θέμα:	ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΘΕΣΗΣ ΑΝΑΛΥΣΗΣ ΕΠΙΠΤΩΣΕΩΝ που συνοδεύει το έγγραφο Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - SWD(2022) 65 final.

συνημμ.: SWD(2022) 65 final

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 22.3.2022
SWD(2022) 65 final

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΘΕΣΗΣ ΑΝΑΛΥΣΗΣ ΕΠΙΠΤΩΣΕΩΝ

που συνοδεύει το έγγραφο

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

{COM(2022) 119 final} - {SWD(2022) 66 final}

Δελτίο συνοπτικής παρουσίασης

Ανάλυση επιπτώσεων ως προς την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

Α. Πολιτικό πλαίσιο

Το στρατηγικό θεματολόγιο του Ευρωπαϊκού Συμβουλίου για την περίοδο 2019-2024 καλεί τα θεσμικά όργανα να προστατεύουν τα δίκτυα πληροφοριών και επικοινωνιών της ΕΕ και τις διαδικασίες λήψης αποφάσεων από κακόβουλες δραστηριότητες κάθε είδους, συμπεριλαμβανομένων των κυβερνοαπειλών και των υβριδικών απειλών. Επακολούθως, το Συμβούλιο Γενικών Υποθέσεων του Δεκεμβρίου 2019 κατέληξε στο συμπέρασμα ότι τα θεσμικά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να αναπτύξουν και να εφαρμόσουν μια ολοκληρωμένη δέσμη μέτρων για τη διασφάλιση της ασφάλειάς τους.

Τον Ιούλιο του 2020 η Επιτροπή ενέκρινε τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας, με την οποία δεσμεύτηκε να συμπληρώσει τις εθνικές προσπάθειες στον τομέα της ασφάλειας. Στο πλαίσιο αυτής της στρατηγικής, η Επιτροπή πρότεινε τη δημιουργία ενός ελάχιστου συνόλου κανόνων για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια σε όλα τα θεσμικά όργανα και τους οργανισμούς της Ένωσης.

Β. Ποιο είναι το πρόβλημα;

Το κύρια προβλήματα είναι τα εξής: i) σημαντικές διαφορές μεταξύ των θεσμικών οργάνων και των οργανισμών της Ένωσης όσον αφορά το επίπεδο ασφαλείας, ανάλογα με τους εσωτερικούς κανόνες τους για την ασφάλεια των πληροφοριών και ii) έλλειψη συντονισμού μεταξύ των θεσμικών οργάνων και των οργανισμών της Ένωσης κατά την εκτέλεση των καθηκόντων τους στον τομέα της ασφάλειας.

Αυτή τη στιγμή τα θεσμικά όργανα και οι οργανισμοί της Ένωσης διαθέτουν δικούς τους κανόνες για την ασφάλεια των πληροφοριών ή δεν έχουν θεσπίσει καν τέτοιους κανόνες. Ο κατακερματισμός του εφαρμοστέου νομικού πλαισίου οδήγησε σε διαφορετικές κατηγορίες μη διαβαθμισμένων πληροφοριών, διαφορετικές σημάνσεις και διαφορετικές οδηγίες χειρισμού. Σε ό,τι αφορά τις διαβαθμισμένες πληροφορίες της ΕΕ, η διαλειτουργικότητα των σχετικών συστημάτων παραμένει περιορισμένη, εμποδίζοντας την απρόσκοπτη διαβίβαση πληροφοριών μεταξύ θεσμικών οργάνων και οργανισμών καθώς και με τα κράτη μέλη.

Η κατάσταση αυτή αυξάνει τον κίνδυνο για παραβιάσεις ασφάλειας στον πιο αδύναμο κρίκο από επιτιθέμενους οι οποίοι θα τον χρησιμοποιήσουν ως αφετηρία για περαιτέρω επιθέσεις κατά άλλων θεσμικών οργάνων ή οργανισμών.

Γ. Τι θα πρέπει να επιτευχθεί;

Γενικός στόχος της πρωτοβουλίας είναι η δημιουργία κανόνων ασφάλειας των πληροφοριών για όλα τα θεσμικά όργανα και τους οργανισμούς της Ένωσης, με στόχο τη διασφάλιση ενισχυμένης και συνεπούς προστασίας από τις εξελισσόμενες απειλές κατά των πληροφοριών τους.

Ο γενικός στόχος μεταφράζεται σε τέσσερις ειδικούς στόχους:

- Θέσπιση εναρμονισμένων και ολοκληρωμένων κατηγοριών πληροφοριών
- Εντοπισμός κενών ασφαλείας και εφαρμογή των απαιτούμενων μέτρων

- Δημιουργία αποδοτικής συνεργασίας σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά όργανα και τους οργανισμούς της Ένωσης
- Εκσυγχρονισμός των πολιτικών ασφάλειας των πληροφοριών, ο οποίος λαμβάνει υπόψη τον ψηφιακό μετασχηματισμό και την τηλεργασία

Δ. Ποιες απόψεις διατύπωσαν τα διάφορα ενδιαφερόμενα μέρη;

Τα ενδιαφερόμενα μέρη των οποίων ζητήθηκε η γνώμη (θεσμικά όργανα και οργανισμοί της Ένωσης, εθνικές αρχές ασφαλείας των κρατών μελών και εμπειρογνώμονες σε θέματα έρευνας από το Κοινό Κέντρο Ερευνών) συμφώνησαν ως προς την ανάγκη κοινών προτύπων για την ασφάλεια των πληροφοριών για όλα τα θεσμικά όργανα και τους οργανισμούς της Ένωσης, με έμφαση στα ακόλουθα σημεία:

- Θα πρέπει να λαμβάνονται υπόψη η ποικιλομορφία και το διαφορετικό επιχειρηματικό περιβάλλον κάθε θεσμικού οργάνου ή οργανισμού και να επιτρέπονται τοπικές λύσεις·
- Αν και τα περισσότερα θεσμικά όργανα και οργανισμοί είναι έτοιμα να συνεργαστούν με τους ομολόγους τους σε κοινούς φορείς για σκοπούς ασφάλειας των πληροφοριών, δεν είναι διατεθειμένα να μεταβιβάσουν τις εξουσίες που διαθέτουν όσον αφορά τη λήψη αποφάσεων·
- Το σχέδιο κανονισμού θα πρέπει να συνταχθεί με βάση τη διακυβερνητική συμφωνία[1] των κρατών μελών για την προστασία διαβαθμισμένων πληροφοριών.

Ε. Ποιος είναι ο αντίκτυπος της πρότασης;

Οφέλη

Με τη δημιουργία βασικού πλαισίου κανόνων όσον αφορά την ασφάλεια των πληροφοριών μεταξύ των θεσμικών οργάνων και των οργανισμών της Ένωσης, το σχέδιο κανονισμού θα αυξήσει τα συνολικά επίπεδα ασφάλειας των πληροφοριών, μειώνοντας παράλληλα τις υφιστάμενες αποκλίσεις. Αναμένεται επίσης να συμβάλει στην εξάλειψη πιθανών αδύναμων κρίκων, προστατεύοντας παράλληλα τις πληροφορίες που ανταλλάσσονται εντός της ευρωπαϊκής διοίκησης.

Από άποψη αποτελεσματικότητας, το σχέδιο κανονισμού αναμένεται να αποφέρει οφέλη μέσα από τη συντονισμένη εκτέλεση των κοινών καθηκόντων όσον αφορά την ασφάλεια των πληροφοριών (π.χ. εξουσιοδοτήσεις, διαπίστευση συστημάτων επικοινωνίας και πληροφοριών) και τη δημιουργία κοινών οργάνων διακυβέρνησης (π.χ. διοργανική ομάδα συντονισμού, τεχνικές υποομάδες).

Οικονομικός αντίκτυπος

Για τα θεσμικά όργανα και τους οργανισμούς της Ένωσης, οι προσπάθειες που απαιτούνται για την εφαρμογή της νέας νομοθεσίας αναμένεται να αντισταθμιστούν από τη βελτίωση της αποτελεσματικότητας, ενώ το πρόσθετο κόστος μπορεί να καλυφθεί στο πλαίσιο των υφιστάμενων προγραμμάτων για τη βελτίωση της ασφάλειας των πληροφοριών που διαθέτει κάθε όργανο ή οργανισμός. Μακροπρόθεσμα, τα θεσμικά όργανα και οι οργανισμοί της Ένωσης θα επωφεληθούν από τη

[1] Συμφωνία των αντιπροσώπων των κρατών μελών της Ευρωπαϊκής Ένωσης, που συνήλθαν στο πλαίσιο του Συμβουλίου, σχετικά με την προστασία διαβαθμισμένων πληροφοριών οι οποίες ανταλλάσσονται προς το συμφέρον της Ευρωπαϊκής Ένωσης, 2011/C202/05.

συνεκτική προσέγγιση ως προς την αντιμετώπιση των διαρκώς εξελισσόμενων απειλών για την ασφάλεια των πληροφοριών.

Η Ευρωπαϊκή Επιτροπή θα πρέπει να εξασφαλίσει τη μόνιμη γραμματεία της διοργανικής ομάδας συντονισμού και να διαθέσει ανθρώπινους πόρους για το έργο αυτό (έναν υπάλληλο AD και έναν υπάλληλο AST).

Δεν αναμένονται οικονομικές επιπτώσεις στο επίπεδο των διοικήσεων των κρατών μελών και του ιδιωτικού τομέα.

Δ. Παρακολούθηση

Πότε θα επανεξεταστεί η πολιτική;

Κάθε 5 έτη μετά την ημερομηνία εφαρμογής θα διενεργείται πλήρης αξιολόγηση, ώστε να αξιολογούνται ο αντίκτυπος και η εφαρμογή του σχεδίου κανονισμού. Η Επιτροπή θα συντάσσει έκθεση με τα πορίσματά της και θα την υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.