Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 10 Ιουνίου 2022
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

ΣΗΜΕΙΩΜΑ ΣΗΜΕΙΟΥ «I/A»

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Επιτροπή των Μονίμων Αντιπροσώπων / Συμβούλιο
αριθ. προηγ. εγγρ.:	9317/2/22 REV 2
Θέμα:	Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με την ειδική έκθεση του Ευρωπαϊκού Ελεγκτικού Συνεδρίου αριθ. 05/2022 «Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ: Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών» - Έγκριση

1. Στις 30 Μαρτίου 2022, το Ευρωπαϊκό Ελεγκτικό Συνέδριο δημοσίευσε την ειδική έκθεση αριθ. 05/2022 με θέμα «Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ: Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών».[1]

2. Κατά τη συνεδρίασή της στις 13 Απριλίου 2022, η Επιτροπή των Μόνιμων Αντιπροσώπων ανέθεσε την εξέταση της ειδικής έκθεσης στην οριζόντια ομάδα για θέματα κυβερνοχώρου.[2]

[1] 8040/22.
[2] 8041/22.

3. Στις 3 Μαΐου 2022, οι εκπρόσωποι του Ελεγκτικού Συνεδρίου παρουσίασαν την ειδική έκθεση στην οριζόντια ομάδα για θέματα κυβερνοχώρου. Μετά τις συζητήσεις σχετικά με την έκθεση κατά την ίδια συνεδρίαση της ομάδας, η Προεδρία εκπόνησε σχέδιο συμπερασμάτων του Συμβουλίου, το οποίο συζητήθηκε από την ομάδα κατά τη συνεδρίασή της στις 24 Μαΐου 2022.

4. Στις 10 Ιουνίου 2022, η οριζόντια ομάδα για θέματα κυβερνοχώρου κατέληξε σε συμφωνία επί του κειμένου που παρατίθεται στο παράρτημα.

5. Η Επιτροπή των Μόνιμων Αντιπροσώπων καλείται να εγκρίνει το εν λόγω σχέδιο συμπερασμάτων και να εισηγηθεί στο Συμβούλιο να το εγκρίνει σε προσεχή σύνοδο.

ΠΑΡΑΡΤΗΜΑ

ΣΧΕΔΙΟ ΣΥΜΠΕΡΑΣΜΑΤΩΝ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με την ειδική έκθεση αριθ. 05/2022 του Ευρωπαϊκού Ελεγκτικού Συνεδρίου «Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ: Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών»

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με τη βελτίωση της εξέτασης των ειδικών εκθέσεων που καταρτίζει το Ελεγκτικό Συνέδριο στα πλαίσια της διαδικασίας απαλλαγής[3]:

1. ΣΗΜΕΙΩΝΕΙ την ειδική έκθεση αριθ. 05/2022 του Ευρωπαϊκού Ελεγκτικού Συνεδρίου με τίτλο «Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ: Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών»[4].

2. ΥΠΟΓΡΑΜΜΙΖΕΙ τη σημασία και την επείγουσα ανάγκη ενίσχυσης του επιπέδου κυβερνοασφάλειας εντός των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, δεδομένης της πρόσφατης εντατικοποίησης του ψηφιακού μετασχηματισμού εντός των θεσμικών οργάνων, των ευαίσθητων πληροφοριών που υφίστανται επεξεργασία, του συνεχώς αυξανόμενου αριθμού και της σοβαρότητας των επιθέσεων κατά των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ και του επιπέδου απειλής που αντιμετωπίζουν.

[3] 7515/00 + COR 1
[4] 8040/22.

3. ΥΠΕΝΘΥΜΙΖΕΙ τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου, της 20ής Ιουνίου 2019[5], στα οποία το Ευρωπαϊκό Συμβούλιο κάλεσε τα θεσμικά όργανα της ΕΕ, μαζί με τα κράτη μέλη, να επεξεργαστούν μέτρα για να αυξηθεί η ανθεκτικότητα και να βελτιωθεί η νοοτροπία ασφαλείας της ΕΕ έναντι των υβριδικών απειλών και των απειλών στον κυβερνοχώρο από σημεία εκτός της ΕΕ, καθώς και να προστατευθούν καλύτερα τα δίκτυα πληροφοριών και επικοινωνιών της ΕΕ, όπως και οι ενωσιακές διαδικασίες λήψης αποφάσεων, από κακόβουλες πράξεις κάθε είδους.

4. ΥΠΕΝΘΥΜΙΖΕΙ τα συμπεράσματά του της 10ης Δεκεμβρίου 2019 σχετικά με συμπληρωματικές προσπάθειες για την ενίσχυση της ανθεκτικότητας και την αντιμετώπιση των υβριδικών απειλών[6], στα οποία κάλεσε τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ, με την υποστήριξη των κρατών μελών, να εξασφαλίσουν την ικανότητα της Ένωσης να προστατεύει την ακεραιότητά της και να ενισχύει την ασφάλεια των δικτύων πληροφοριών και επικοινωνιών της ΕΕ και τις διαδικασίες λήψης αποφάσεων από κακόβουλες δραστηριότητες κάθε είδους, βάσει ολοκληρωμένης αξιολόγησης των απειλών. Προς τον σκοπό αυτό, στα συμπεράσματα αναφερόταν ότι τα θεσμικά και λοιπά όργανα και οι οργανισμοί, με την υποστήριξη των κρατών μελών, θα πρέπει να αναπτύξουν και να εφαρμόσουν μια ολοκληρωμένη δέσμη μέτρων για να εγγυηθούν την ασφάλειά τους, σύμφωνα με την εντολή του Ευρωπαϊκού Συμβουλίου του Ιουνίου του 2019[7].

5. ΥΠΕΝΘΥΜΙΖΕΙ τα συμπεράσματά του της 22ας Μαρτίου 2021 σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[8], όπου τόνισε η κυβερνοασφάλεια και το παγκόσμιο και ανοικτό διαδίκτυο είναι ζωτικής σημασίας για τη λειτουργία της δημόσιας διοίκησης και των θεσμών τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο, καθώς και για την κοινωνία και την οικονομία μας στο σύνολό της.

---

5 EUCO 9/19
6 14972/19.
7 EUCO 9/19
8 6722/21.

6. ΥΠΕΝΘΥΜΙΖΕΙ τα συμπεράσματά του, της 23ης Μαΐου 2022, σχετικά με την ανάπτυξη της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο[9], στα οποία παροτρύνονται τα θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ να προβούν σε χαρτογράφηση των υφιστάμενων εργαλείων ασφαλούς επικοινωνίας στον τομέα του κυβερνοχώρου, η οποία θα συζητηθεί στα αρμόδια όργανα του Συμβουλίου και με τις αρμόδιες ομάδες συνεργασίας, όπως το δίκτυο CSIRT και το EU CyCLONe.

7. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη να αντιμετωπιστεί ο συστημικός κίνδυνος που υφίσταται στη διασύνδεση μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ καθώς και μεταξύ αυτών και των θεσμικών οργάνων των κρατών μελών, παρά τη θεσμική ανεξαρτησία και τη διοικητική αυτονομία τους.

8. ΣΗΜΕΙΩΝΕΙ τις παρατηρήσεις της ειδικής έκθεσης, δηλαδή ότι τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ δεν έχουν επιτύχει επίπεδο ετοιμότητας στον κυβερνοχώρο ανάλογο προς τις απειλές και έχουν διαφορετικά επίπεδα ωριμότητας ως προς την κυβερνοασφάλεια. ΑΝΑΓΝΩΡΙΖΕΙ ότι θα πρέπει να βελτιωθεί το επίπεδο ετοιμότητας των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ στον τομέα της κυβερνοασφάλειας καθώς και οι μεταξύ τους συνέργειες.

9. ΕΝΘΑΡΡΥΝΕΙ, ως εκ τούτου, τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ να συνεχίσουν την εφαρμογή μέτρων διαχείρισης κινδύνων στον κυβερνοχώρο που διασφαλίζουν ανάλογο επίπεδο κυβερνοασφάλειας, όπως προβλέπεται στην προτεινόμενη οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, με την οποία καταργείται η οδηγία (ΕΕ) 2016/1148, προκειμένου να βελτιωθεί το επίπεδο ετοιμότητάς τους.

10. ΚΑΛΕΙ τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ να εντείνουν τόσο τις προσπάθειές τους για την προστασία τους από κυβερνοαπειλές όσο και τη συνεργασία τους για τη θέσπιση συνεκτικών προτύπων και προδιαγραφών, ιδίως για τις δημόσιες συμβάσεις, τα έργα και τις υπηρεσίες που σχετίζονται με την κυβερνοασφάλεια, και να βελτιώσουν τη διαλειτουργικότητα των οικείων συστημάτων ΤΠ, μεταξύ άλλων με σκοπό τη διασφάλιση της ασφαλούς επικοινωνίας μη διαβαθμισμένου περιεχομένου.

---

9 9364/22.

11. ΚΑΛΕΙ τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και την ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ (CERT-ΕΕ), στο πλαίσιο των αρμοδιοτήτων τους, να εντείνουν τη συνεργασία τους για τη στήριξη των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ στις προσπάθειές τους στον τομέα της κυβερνοασφάλειας, ιδίως όσον αφορά την ανάπτυξη ικανοτήτων για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ που έχουν χαμηλότερο επίπεδο ωριμότητας ως προς την κυβερνοασφάλεια.

12. ΣΗΜΕΙΩΝΕΙ τα συμπεράσματα και τις συστάσεις της ειδικής έκθεσης και ΑΝΑΓΝΩΡΙΖΕΙ ότι θα πρέπει να βελτιωθεί σημαντικά το επίπεδο ετοιμότητας των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ στον τομέα της κυβερνοασφάλειας καθώς και οι μεταξύ τους συνέργειες. Τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διαθέτουν ένα ολοκληρωμένο πλαίσιο διαχείρισης κινδύνων για την κυβερνοασφάλεια, να διενεργούν τακτικές εκτιμήσεις κινδύνου και ελέγχους, βάσει κοινής ή ευρέως γνωστής μεθοδολογίας και διεθνών προτύπων, και να συστηματοποιούν προγράμματα ευαισθητοποίησης και κατάρτισης του προσωπικού στον τομέα της κυβερνοασφάλειας.

3. ΕΠΙΣΗΜΑΙΝΕΙ επίσης ότι τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διαθέτουν επαρκή προϋπολογισμό για τη διασφάλιση της εφαρμογής μέτρων προστασίας από κυβερνοαπειλές, τηρώντας παράλληλα το πολυετές δημοσιονομικό πλαίσιο, και ΣΗΜΕΙΩΝΕΙ τη σύσταση της ειδικής έκθεσης ότι θα πρέπει να οριστεί όργανο που να εκπροσωπεί όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ, και να διαθέτει την κατάλληλη εντολή και τα κατάλληλα μέσα για την παρακολούθηση της συμμόρφωσης με τους κοινούς κανόνες για την κυβερνοασφάλεια.

14. ΑΝΑΓΝΩΡΙΖΕΙ ότι η CERT-ΕΕ θα πρέπει να ενημερώνεται χωρίς καθυστέρηση για σημαντικά συμβάντα στον κυβερνοχώρο εντός των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ και, για τον σκοπό αυτό, θα πρέπει να διαθέτει επαρκείς πόρους που να είναι προβλέψιμοι και προσαρμοσμένοι στο εκάστοτε επίπεδο απειλής και τις ανάγκες των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, ιδίως όσον αφορά το προσωπικό, τον τεχνικό εξοπλισμό και τις υποδομές.

15. ΣΗΜΕΙΩΝΕΙ ότι θα πρέπει να ενισχυθούν και να συστηματοποιηθούν η συνεργασία και η ανταλλαγή πληροφοριών σχετικά με την κυβερνοασφάλεια καθώς και η διαλειτουργικότητα ασφαλών διαύλων επικοινωνίας μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. ΖΗΤΕΙ η εν λόγω συνεργασία και ανταλλαγή πληροφοριών να περιλαμβάνει επίσης τις δημόσιες αρχές που είναι αρμόδιες για την κυβερνοασφάλεια στα κράτη μέλη.

16. ΣΗΜΕΙΩΝΕΙ τις απαντήσεις της Επιτροπής, της CERT-ΕΕ και του ENISA που συνοδεύουν την ειδική έκθεση.

17. ΚΑΛΕΙ την Επιτροπή να λάβει υπόψη τις συστάσεις της ειδικής έκθεσης και να είναι φιλόδοξη κατά τον σχεδιασμό των πολιτικών κυβερνοασφάλειας των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, καθώς και να υποστηρίξει περισσότερες συνέργειες μεταξύ τους.