Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 20 Μαρτίου 2019
(OR. en)

7737/19

CYBER 101	**RELEX 287**
COPEN 118	**TELECOM 141**
COPS 92	**DAPIX 109**
COSI 52	**CATS 43**
DATAPROTECT 98	**CSC 111**
IND 102	**CSCI 47**
JAI 313	**IA 106**
JAIEX 44	**EJUSTICE 44**
POLMIL 31	

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	19 Μαρτίου 2019
Αποδέκτης:	Αντιπροσωπίες
αριθ. προηγ. εγγρ.:	6866/19
Θέμα:	Συμπεράσματα του Συμβουλίου σχετικά με την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ

Επισυνάπτονται στο παράρτημα για τις αντιπροσωπίες τα συμπεράσματα του Συμβουλίου σχετικά με την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ τα οποία υιοθετήθηκαν από το Συμβούλιο Γενικών Υποθέσεων της 19ης Μαρτίου 2019.

ΠΑΡΑΡΤΗΜΑ

Συμπεράσματα του Συμβουλίου σχετικά με την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ

Το Συμβούλιο της Ευρωπαϊκής Ένωσης,

1. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του για την ανθεκτικότητα, την αποτροπή και την άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ[1],

2. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματα του Συμβουλίου για τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο[2],

3. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματα του Συμβουλίου για την ανάπτυξη εξωτερικών ικανοτήτων στον κυβερνοχώρο[3],

4. ΕΠΑΝΑΛΑΜΒΑΝΟΝΤΑΣ ότι για να επιτευχθεί υψηλό επίπεδο ασφάλειας των συστημάτων δικτύων και πληροφοριών απαιτείται να ενισχυθούν οι ικανότητες και οι δυνατότητες κυβερνοασφάλειας, και στη συνέχεια και η κυβερνοανθεκτικότητα των κρατών μελών και των θεσμικών, λοιπών οργάνων και οργανισμών της ΕΕ,

5. ΕΚΦΡΑΖΟΝΤΑΣ ικανοποίηση για την πρόοδο που έχουν επιτύχει τα κράτη μέλη ως προς την ενίσχυση των ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT),

6. ΧΑΙΡΕΤΙΖΟΝΤΑΣ την ίδρυση του δικτύου CSIRT από τα κράτη μέλη, με την ενεργό υποστήριξη της Επιτροπής και του ENISA, καθώς και την ενισχυμένη συνεργασία σε στρατηγικό επίπεδο μέσω της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS) που αποτελείται από αντιπροσώπους των κρατών μελών, την Επιτροπής και του ENISA.

---

1 14435/17 (Συμπεράσματα του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, της 20ής Νοεμβρίου 2017)

2 10086/18 (Σχέδιο συμπερασμάτων του Συμβουλίου για τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο, της 26ης Ιουνίου 2018)

3 10496/18 (Συμπεράσματα του Συμβουλίου σχετικά με κατευθυντήριες γραμμές για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο, της 26ης Ιουνίου 2018)

7. ΤΟΝΙΖΟΝΤΑΣ τον κεντρικό ρόλο που διαδραματίζει η ομάδα συνεργασίας NIS στην παροχή της αναγκαίας καθοδήγησης ώστε να εναρμονιστεί όσο το δυνατόν περισσότερο σε ολόκληρη την ΕΕ η προσέγγιση που θα ακολουθηθεί κατά τη μεταφορά της οδηγίας NIS[4] στο εθνικό δίκαιο, και προκειμένου να αντιμετωπιστούν τα συναφή ζητήματα κυβερνοασφάλειας,

8. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ την υφιστάμενη στήριξη που παρέχει επί του παρόντος η Επιτροπή στα κράτη μέλη για ανάπτυξη ικανοτήτων CSIRT μέσω του μηχανισμού «Συνδέοντας την Ευρώπη»,

9. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ τη στήριξη που παρέχεται στις αρχές επιβολής του νόμου για την οικοδόμηση ικανοτήτων στην καταπολέμηση του κυβερνοεγκλήματος, μέσω του Ταμείου Εσωτερικής Ασφάλειας και του CEPOL,

10. ΧΑΙΡΕΤΙΖΟΝΤΑΣ την επικαιροποίηση του πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα με στόχο να υποστηριχθεί περαιτέρω η ανάπτυξη των ικανοτήτων κυβερνοάμυνας των κρατών μελών,

11. ΕΠΙΔΟΚΙΜΑΖΟΝΤΑΣ την πρόοδο που έχει επιτευχθεί στην εφαρμογή της οδηγίας NIS από τα κράτη μέλη,

12. ΕΠΙΣΗΜΑΙΝΟΝΤΑΣ ότι η κυβερνοασφάλεια είναι ένας σύνθετος, αλληλεξαρτώμενος και διαρκώς μεταβαλλόμενος τομέας που απαιτεί την προσαρμογή του πολιτικού και νομικού πλαισίου στις νέες τεχνολογικές τάσεις και στις αναδυόμενες τεχνολογίες, όπως στην τεχνητή νοημοσύνη, την τεχνολογία αλυσίδας συστοιχιών (blockchain) και την κβαντική υπολογιστική,

---

[4] 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 (ΕΕ L 194 της 19.7.2016).

13. ΤΟΝΙΖΟΝΤΑΣ ότι τα προγράμματα κατάρτισης και εκπαίδευσης σχετικά με την κυβερνοασφάλεια, καθώς και η ενημέρωση και ευαισθητοποίηση των τελικών χρηστών όσον αφορά τις απειλές κατά της ασφάλειας είναι καθοριστικά για τη μείωση των κινδύνων κατά της κυβερνοασφάλειας,

14. ΥΠΟΓΡΑΜΜΙΖΟΝΤΑΣ ότι οι κυβερνοασκήσεις συνιστούν αποτελεσματικά εργαλεία για την αξιολόγηση και την περαιτέρω βελτίωση του επιπέδου ετοιμότητας της ΕΕ και των κρατών μελών της όσον αφορά την αντιμετώπιση συμβάντων και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας,

15. ΕΠΑΝΑΛΑΜΒΑΝΟΝΤΑΣ ότι ο κυβερνοχώρος δεν έχει σύνορα, με αποτέλεσμα οι διασυνοριακές και διατομεακές προοπτικές και η συναφής συνεργασία να αποτελούν ακλόνητη αρχή των δραστηριοτήτων και των πρωτοβουλιών οικοδόμησης κυβερνοϊκανοτήτων,

16. ΤΟΝΙΖΟΝΤΑΣ τη σημασία της συνεργασίας μεταξύ του δημόσιου τομέα, του ιδιωτικού τομέα και του ακαδημαϊκού χώρου, ιδίως μέσω συνεργατικών σχεδίων,

17. ΤΟΝΙΖΟΝΤΑΣ τη σημασία της συνεργασίας μεταξύ μη στρατιωτικού και στρατιωτικού τομέα για την επίτευξη κοινών στόχων στον τομέα του κυβερνοχώρου με στόχο να εξασφαλιστεί μια συνεκτική και αποτελεσματική αντιμετώπιση των κυβερνοαπειλών,

18. ΣΗΜΕΙΩΝΕΙ την πρόοδο που έχει επιτευχθεί από ομάδα κρατών μελών όσον αφορά την ανάπτυξη ομάδων ταχείας αντίδρασης στον κυβερνοχώρο με σκοπό την εμβάθυνση της εθελοντικής συνεργασίας στον τομέα του κυβερνοχώρου μέσω αμοιβαίας συνδρομής,

19. ΧΑΙΡΕΤΙΖΕΙ τις συζητήσεις που βρίσκονται σε εξέλιξη στο Συμβούλιο σχετικά με την πρόταση της Επιτροπής για κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη σύσταση του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού,

20. ΕΝΘΑΡΡΥΝΕΙ την ενεργό συμμετοχή στις τρέχουσες εργασίες της ομάδας συνεργασίας NIS, ιδίως σε ό,τι αφορά τη δημιουργία κυβερνοϊκανοτήτων,

21. ΕΝΘΑΡΡΥΝΕΙ το συνεχιζόμενο έργο της ομάδας συνεργασίας NIS για τη συντονισμένη αντιμετώπιση σε ενωσιακό επίπεδο συμβάντων και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας,

22. ΚΑΛΕΙ τα κράτη μέλη να αναπτύξουν περαιτέρω τις εθνικές τους στρατηγικές για την κυβερνοασφάλεια και να συνεκτιμούν τη διάσταση της κυβερνοασφάλειας, λαμβάνοντας, υπόψη τις ειδικές ανά τομέα απαιτήσεις,

23. ΚΑΛΕΙ τα κράτη μέλη να διενεργούν συνεχή παρακολούθηση, αξιολόγηση/αποτίμηση του αντίκτυπου των μέτρων που έχουν ληφθεί για την ενίσχυση της κυβερνοανθεκτικότητας και να ενισχύουν σε εθνικό επίπεδο τις ικανότητες και τις δυνατότητές τους στον κυβερνοχώρο,

24. ΚΑΛΕΙ τα κράτη μέλη να ενσωματώσουν την κυβερνοασφάλεια και τον ψηφιακό γραμματισμό στα προγράμματα σπουδών όλων των βαθμίδων της εκπαίδευσης (πρωτοβάθμια, δευτεροβάθμια, τριτοβάθμια και διά βίου μάθηση) με βάση, κατά περίπτωση, ήδη υπάρχοντα και μελλοντικά επαγγέλματα,

25. ΚΑΛΕΙ τα κράτη μέλη να υλοποιήσουν πρωτοβουλίες ευαισθητοποίησης του κοινού και των τελικών χρηστών ως προς την κυβερνοασφάλεια και κυβερνοϋγιεινή, οι οποίες θα στοχεύουν στους εργαζόμενους του δημόσιου τομέα,

26. ΠΡΟΤΡΕΠΕΙ τα κράτη μέλη να διεξαγάγουν ασκήσεις για την κυβερνοασφάλεια σε εθνικό επίπεδο, καθώς και να διεξαγάγουν και/ή να συμμετάσχουν σε ασκήσεις κυβερνοασφάλειας σε ενωσιακό επίπεδο προκειμένου να πραγματοποιήσουν δοκιμές και να καταρτιστούν όσον αφορά τις στρατηγικές και τεχνολογικές πτυχές, καθώς και για να αναπτύξουν ουσιαστικά και στην πράξη τις απαιτούμενες δεξιότητες,

27. ΚΑΛΕΙ τα κράτη μέλη να αναπτύξουν περαιτέρω τις τεχνικές και επιχειρησιακές ικανότητες των CSIRT τους στον τομέα της κυβερνοασφάλειας, όσον αφορά την πρόληψη, τον μετριασμό και την αντιμετώπιση συμβάντων,

28. ΖΗΤΕΙ από την Επιτροπή και τον ENISA να συνεχίσουν να υποστηρίζουν τα κράτη μέλη όσον αφορά την ανάπτυξη των ικανοτήτων και δυνατοτήτων του δικτύου των CSIRT τους, έτσι ώστε αυτά να μπορούν να συνεργάζονται καλύτερα, να ανταλλάσσουν πληροφορίες σχετικά με συμβάντα και να αντιμετωπίζουν με αποτελεσματικότητα διασυνοριακά περιστατικά μεγάλης κλίμακας,

29. ΚΑΛΕΙ τα κράτη μέλη να συνεχίσουν να βοηθούν τις αρχές επιβολής του νόμου να αναπτύξουν συγκεκριμένες ικανότητες σε συντονισμό με τις αρμόδιες ευρωπαϊκές αρχές, με σκοπό την αποτελεσματική καταπολέμηση του κυβερνοεγκλήματος σε ενωσιακό επίπεδο,

30. ΚΑΛΕΙ τα κράτη μέλη να αυξήσουν τις επενδύσεις για τη οικοδόμηση κυβερνοϊκανοτήτων,

31. ΖΗΤΕΙ από την Επιτροπή και τον ENISA να υλοποιήσουν προγράμματα ευαισθητοποίησης και να παράσχουν κατάρτιση σχετικά με την κυβερνοασφάλεια στους εργαζόμενους των θεσμικών και λοιπών οργάνων και των οργανισμών της ΕΕ,

32. ΖΗΤΕΙ από την ΕΕ και τα κράτη μέλη να ανταλλάσσουν πληροφορίες και βέλτιστες πρακτικές σε εθελοντική βάση, προκειμένου να συμβάλλουν στον εντοπισμό και την κάλυψη των βασικών αναγκών οικοδόμησης κυβερνοϊκανοτήτων σε εθνικό και ενωσιακό επίπεδο,

33. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να υποστηρίξουν την έρευνα για την κυβερνοασφάλεια και να προωθήσουν την κυβερνοασφάλεια ως ζήτημα σε άλλους τομείς σπουδών, συνδυάζοντας διάφορους κλάδους της έρευνας και ανάπτυξης σχετικά με την κυβερνοασφάλεια σε ένα ολοκληρωμένο σύνολο, και να προωθήσουν την αριστεία στην έρευνα για την κυβερνοασφάλεια,

34. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να αναπτύξουν έρευνα για την κυβερνοασφάλεια που θα αντικατοπτρίζει τις κοινωνιακές ανάγκες και να ενσωματώσουν τα αποτελέσματα της έρευνας στην αγορά,

35. ΖΗΤΕΙ από την ΕΕ και τα κράτη μέλη της να λαμβάνουν υπόψη την κυβερνοασφάλεια κατά τη σύναψη συμβάσεων ΤΠΕ, κατά περίπτωση.