Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 22 Μαρτίου 2022
(OR. en)

Διοργανικός φάκελος:
2022/0085(COD)

7474/22
ADD 1

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

ΠΡΟΤΑΣΗ

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.:	COM(2022) 122 final - Annexes 1 to 2
Θέμα:	ΠΑΡΑΡΤΗΜΑΤΑ της Πρότασης ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - COM(2022) 122 final - Annexes 1 to 2.

συνημμ.: COM(2022) 122 final - Annexes 1 to 2

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ΠΑΡΑΡΤΗΜΑΤΑ

της

Πρότασης ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ΠΑΡΑΡΤΗΜΑ Ι

Στη βασική δέσμη κανόνων κυβερνοασφάλειας λαμβάνονται υπόψη οι ακόλουθοι τομείς:

(1) πολιτική κυβερνοασφάλειας, συμπεριλαμβανομένων των στόχων και των προτεραιοτήτων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ιδίως όσον αφορά τη χρήση υπηρεσιών νεφοϋπολογιστικής (κατά την έννοια του άρθρου 4 παράγραφος 19 της οδηγίας [πρόταση οδηγίας NIS 2]) και τις τεχνικές ρυθμίσεις που καθιστούν δυνατή την τηλεργασία·

(2) οργάνωση της κυβερνοασφάλειας, συμπεριλαμβανομένου του καθορισμού ρόλων και αρμοδιοτήτων·

(3) διαχείριση περιουσιακών στοιχείων, συμπεριλαμβανομένης της απογραφής περιουσιακών στοιχείων ΤΠ και της χαρτογράφησης του δικτύου ΤΠ·

(4) έλεγχος πρόσβασης·

(5) ασφάλεια επιχειρήσεων·

(6) ασφάλεια επικοινωνιών·

(7) απόκτηση, ανάπτυξη και συντήρηση συστημάτων·

(8) σχέσεις με προμηθευτές·

(9) διαχείριση περιστατικών, συμπεριλαμβανομένων προσεγγίσεων για τη βελτίωση της ετοιμότητας, της αντιμετώπισης και της αποκατάστασης σε σχέση με περιστατικά, και συνεργασία με τη CERT-ΕΕ, π.χ. διατήρηση της παρακολούθησης της ασφάλειας και της καταγραφής·

(10) διαχείριση της επιχειρησιακής συνέχειας και διαχείριση κρίσεων· και

(11) προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης στον τομέα της κυβερνοασφάλειας.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης εξετάζουν τουλάχιστον τα ακόλουθα ειδικά μέτρα κυβερνοασφάλειας κατά την εφαρμογή της βασικής δέσμης κανόνων κυβερνοασφάλειας και στα σχέδιά τους για την κυβερνοασφάλεια, σύμφωνα με τα έγγραφα καθοδήγησης και τις συστάσεις του ΙΙCB:

(1) συγκεκριμένα μέτρα για τη μετάβαση προς την αρχιτεκτονική μηδενικής εμπιστοσύνης (ήτοι ένα μοντέλο ασφάλειας, ένα σύνολο αρχών σχεδιασμού συστήματος και μια συντονισμένη στρατηγική κυβερνοασφάλειας και διαχείρισης συστήματος με βάση την αναγνώριση της ύπαρξης απειλών τόσο εντός όσο και εκτός των παραδοσιακών ορίων του δικτύου)·

(2) εφαρμογή, κατά κανόνα, της πολυπαραγοντικής επαλήθευσης ταυτότητας σε όλα τα συστήματα δικτύου και πληροφοριών·

(3) επίτευξη ασφάλειας στην αλυσίδα εφοδιασμού λογισμικού μέσω κριτηρίων για την ασφαλή ανάπτυξη και αξιολόγηση λογισμικού·

(4) ενίσχυση των κανόνων για τη σύναψη συμβάσεων ώστε να διευκολυνθεί η επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας μέσω:

α) της άρσης των συμβατικών φραγμών που περιορίζουν την κοινοποίηση από τους παρόχους υπηρεσιών ΤΠ στη CERT-ΕΕ πληροφοριών σχετικά με περιστατικά, τρωτά σημεία και κυβερνοαπειλές·

β) της συμβατικής υποχρέωσης υποβολής εκθέσεων για περιστατικά, τρωτά σημεία και κυβερνοαπειλές, καθώς και εφαρμογής κατάλληλης αντιμετώπισης και παρακολούθησης περιστατικών.