Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 22 Μαρτίου 2022
(OR. en)

7474/22

Διοργανικός φάκελος:
2022/0085 (COD)

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
Θέμα:	Πρόταση 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.

συνημμ.: COM(2022) 122 final

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ 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}

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ

• Αιτιολόγηση και στόχοι της πρότασης

Με την παρούσα πρόταση θεσπίζεται πλαίσιο διασφάλισης κοινών κανόνων και μέτρων κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Η πρόταση αποσκοπεί στην περαιτέρω βελτίωση της ανθεκτικότητας και των ικανοτήτων αντιμετώπισης περιστατικών όλων των οντοτήτων. Η πρόταση συνάδει με τις προτεραιότητες της Επιτροπής να προετοιμάσει την Ευρώπη για την ψηφιακή εποχή και να οικοδομήσει μια οικονομία έτοιμη να αντιμετωπίσει το μέλλον, στην υπηρεσία των πολιτών. Επιπλέον, η διασφάλιση ασφαλούς και ανθεκτικής δημόσιας διοίκησης αποτελεί ακρογωνιαίο λίθο του ψηφιακού μετασχηματισμού της κοινωνίας στο σύνολό της.

Η παρούσα πρόταση βασίζεται στη στρατηγική της ΕΕ για την Ένωση Ασφάλειας [COM(2020) 605 final] και στη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία [JOIN(2020) 18 final].

Με την πρόταση εκσυγχρονίζεται το υφιστάμενο νομικό πλαίσιο για τη CERT-ΕΕ και λαμβάνονται υπόψη η μεταβολή και η αύξηση της ψηφιοποίησης των θεσμικών και λοιπών οργάνων και των οργανισμών κατά τα πρόσφατα έτη, καθώς και το εξελισσόμενο τοπίο των απειλών κατά της κυβερνοασφάλειας. Και οι δύο εξελίξεις εντάθηκαν περαιτέρω αφότου ξεκίνησε η κρίση λόγω της νόσου COVID-19, ενώ ο αριθμός των περιστατικών εξακολουθεί να αυξάνεται, καθώς εξαπολύονται ολοένα και πιο εξελιγμένες επιθέσεις από ένα ευρύ φάσμα πηγών.

Η πρόταση μετονομάζει τη CERT-ΕΕ από «ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική» σε «Κέντρο Κυβερνοασφάλειας» για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, σύμφωνα με τις εξελίξεις στα κράτη μέλη και παγκοσμίως, όπου πολλές CERT μετονομάζονται σε κέντρα κυβερνοασφάλειας, αλλά διατηρεί τη σύντομη ονομασία «CERT-ΕΕ» λόγω της αναγνώρισης της ονομασίας.

• Συνέπεια με τις ισχύουσες διατάξεις στον τομέα πολιτικής

Στόχος της παρούσας πρότασης είναι η αύξηση της ανθεκτικότητας των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης στον τομέα της κυβερνοασφάλειας έναντι των κυβερνοαπειλών, καθώς και η διασφάλιση της εναρμόνισης με την ισχύουσα νομοθεσία:

- Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. Εναρμονίζεται επίσης με την πρόταση οδηγίας (ΕΕ) XXXX/XXXX σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (στο εξής: πρόταση οδηγίας NIS 2).

- Κανονισμός (ΕΕ) 2019/881 σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών (πράξη για την κυβερνοασφάλεια).

- Πρόταση κανονισμού (ΕΕ) XXXX/XXXX σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

- Σύσταση της Επιτροπής, της 23ης Ιουνίου 2021, σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας.

- Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

Στο παράρτημα της σύστασης (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο παρατίθεται το προσχέδιο συντονισμένης αντιμετώπισης διασυνοριακών περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

Στο ψήφισμα της 9ης Μαρτίου 2021, το Συμβούλιο της Ευρωπαϊκής Ένωσης επισήμανε ότι η κυβερνοασφάλεια έχει ζωτική σημασία για τη λειτουργία της δημόσιας διοίκησης τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο, καθώς και για την κοινωνία και την οικονομία συνολικά, και τόνισε πόσο σημαντική είναι η ύπαρξη ενός ισχυρού και συνεκτικού πλαισίου ασφάλειας για την προστασία του συνόλου του προσωπικού, των δεδομένων, των δικτύων επικοινωνίας, των συστημάτων πληροφοριών και των διαδικασιών λήψης αποφάσεων της ΕΕ. Πιο συγκεκριμένα, αυτό θα επιτευχθεί με την ενίσχυση της ανθεκτικότητας και τη βελτίωση της νοοτροπίας ασφάλειας των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Θα διατεθούν επαρκείς πόροι και ικανότητες, μεταξύ άλλων στο πλαίσιο ενίσχυσης της εντολής της CERT-ΕΕ.

2. ΝΟΜΙΚΗ ΒΑΣΗ, ΕΠΙΚΟΥΡΙΚΟΤΗΤΑ ΚΑΙ ΑΝΑΛΟΓΙΚΟΤΗΤΑ

- **Νομική βάση**

Η νομική βάση για τον παρόντα κανονισμό είναι το άρθρο 298 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (στο εξής: ΣΛΕΕ) που προβλέπει ότι κατά την εκπλήρωση της αποστολής τους, τα θεσμικά και λοιπά όργανα και οι οργανισμοί της Ένωσης στηρίζονται σε ευρωπαϊκή διοίκηση ανοικτή, αποτελεσματική και ανεξάρτητη. Τηρουμένου του κανονισμού υπηρεσιακής κατάστασης και του καθεστώτος που θεσπίζονται βάσει του άρθρου 336, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αποφασίζοντας μέσω κανονισμών σύμφωνα με τη συνήθη νομοθετική διαδικασία, καθορίζουν τις διατάξεις προς τον σκοπό αυτό.

Η τεχνολογία πληροφοριών έχει παράσχει νέους τρόπους εργασίας, αλληλεπίδρασης με τους πολίτες και βελτίωσης των συνολικών δραστηριοτήτων για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Καθώς η τεχνολογία εξακολουθεί να εξελίσσεται, το τοπίο των κυβερνοαπειλών εξελίσσεται παράλληλα με αυτήν. Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης έχουν καταστεί ιδιαίτερα ελκυστικοί στόχοι εξελιγμένων κυβερνοεπιθέσεων. Η θέσπιση συστημάτων και απαιτήσεων για τη διασφάλιση της κυβερνοασφάλειας φαίνεται να συμβάλει στην αποτελεσματικότητα και την ανεξαρτησία της ευρωπαϊκής διοίκησης, ώστε τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης να μπορούν να λειτουργούν με αποτελεσματικότερο τρόπο σε έναν ψηφιακό κόσμο κατά την εκτέλεση των αποστολών τους.

Επιπλέον, όπως επεξηγείται στο τμήμα 3 κατωτέρω, οι τρέχουσες διαφορές όσον αφορά τη στάση και την προσέγγιση των διαφόρων θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης έναντι της κυβερνοασφάλειας αποτελούν περαιτέρω εμπόδια για μια ανοικτή, αποτελεσματική και ανεξάρτητη ευρωπαϊκή διοίκηση. Χωρίς κοινή προσέγγιση, η στάση των διαφόρων θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης όσον αφορά την κυβερνοασφάλεια θα εξακολουθεί να κινείται σε διαφορετικές κατευθύνσεις. Ως εκ τούτου, η παρούσα νομική βάση είναι κατάλληλη, δεδομένου ότι ο κανονισμός αποσκοπεί στη δημιουργία κοινού νομικού πλαισίου για την κυβερνοασφάλεια εντός των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

- **Επικουρικότητα**

Ο κανονισμός για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης εμπίπτει στην αποκλειστική αρμοδιότητα της Ένωσης.

- **Αναλογικότητα**

Οι κανόνες που προτείνονται στον παρόντα κανονισμό δεν υπερβαίνουν τα αναγκαία για την ικανοποιητική επίτευξη των ειδικών στόχων. Τα προβλεπόμενα μέτρα θα συμβάλουν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας χωρίς να υπερβαίνουν τα αναγκαία για την επίτευξη του στόχου, δεδομένων των διαρκώς αυξανόμενων κινδύνων που πρέπει να αντιμετωπιστούν.

- **Επιλογή της νομικής πράξης**

Η επιλογή κανονισμού, ο οποίος είναι άμεσα εφαρμοστέος, θεωρείται το κατάλληλο νομικό μέσο για τον καθορισμό και τον εξορθολογισμό των υποχρεώσεων που επιβάλλονται στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Για να παρασχεθεί η δυνατότητα για στοχευμένες βελτιώσεις, η πλέον ενδεδειγμένη νομική πράξη είναι ο κανονισμός.

3. ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΚ ΤΩΝ ΠΡΟΤΕΡΩΝ ΑΞΙΟΛΟΓΗΣΕΩΝ, ΤΩΝ ΔΙΑΒΟΥΛΕΥΣΕΩΝ ΜΕ ΤΑ ΕΝΔΙΑΦΕΡΟΜΕΝΑ ΜΕΡΗ ΚΑΙ ΤΩΝ ΕΚΤΙΜΗΣΕΩΝ ΕΠΙΠΤΩΣΕΩΝ

- **Εκ των προτέρων αξιολογήσεις**

Η CERT-EE διενήργησε εκτίμηση των κυριότερων κυβερνοαπειλών στις οποίες τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης είναι εκτεθειμένα επί του παρόντος ή είναι πιθανό να εκτεθούν στο άμεσο μέλλον.

Στην ανάλυση χρησιμοποιήθηκαν τρεις κατηγορίες παρατηρήσεων:

- Απόπειρες παραβίασης των υποδομών ΤΠ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης (εάν είναι επιτυχείς, αντιμετωπίζονται ως περιστατικά, ενώ στις υπόλοιπες περιπτώσεις καταγράφονται ως εντοπισθείσες απόπειρες).

- Απειλές που εντοπίζονται πλησίον των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης (π.χ. σε συναφείς τομείς τους, σε κοινότητες των ενδιαφερόμενων μερών τους ή στην Ευρώπη).

- Σημαντικές τάσεις ως προς τις απειλές που παρατηρούνται παγκόσμια.

Επιπροσθέτως, στην ανάλυση συνυπολογίστηκε το πώς σημαντικές συνεχιζόμενες αλλαγές επηρεάζουν τους τρόπους με τους οποίους τα θεσμικά όργανα της Ένωσης διαχειρίζονται και χρησιμοποιούν τις υποδομές ΤΠ και τις υπηρεσίες τους. Στις αλλαγές αυτές περιλαμβάνονται τα εξής:

- Η αύξηση της τηλεργασίας.
- Η μετάβαση των συστημάτων στο υπολογιστικό νέφος.
- Η αύξηση της εξωτερικής ανάθεσης υπηρεσιών ΤΠ.

Από το 2019 έως το 2021, ο αριθμός των σημαντικών περιστατικών[1] που επηρέασαν τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και πραγματοποιήθηκαν από παράγοντες προηγμένων επίμονων απειλών (advanced persistent threat – APT) αυξήθηκε κατακόρυφα. Ο αριθμός των σημαντικών περιστατικών που σημειώθηκαν κατά το πρώτο εξάμηνο του 2021 ήταν αντίστοιχος του αριθμού που καταγράφηκε ολόκληρο το 2020. Αυτό αντικατοπτρίζεται επίσης στον αριθμό των εικόνων εγκληματολογικής έρευνας (στιγμιότυπα του περιεχομένου των επηρεαζόμενων συστημάτων ή συσκευών) της CERT-ΕΕ που αναλύθηκαν το 2020, ο οποίος τριπλασιάστηκε σε σύγκριση με το 2019, ενώ ο αριθμός των σημαντικών περιστατικών υπερδεκαπλασιάστηκε από το 2018.

Το 2020, η διοικούσα επιτροπή της CERT-ΕΕ έθεσε νέο στρατηγικό στόχο βάσει του οποίου η CERT-ΕΕ θα διασφαλίσει ολοκληρωμένο επίπεδο κυβερνοάμυνας για όλα τα θεσμικά και λοιπά όργανα και οργανισμούς, το οποίο θα διαθέτει κατάλληλο εύρος και βάθος και θα προσαρμόζεται διαρκώς στις τρέχουσες ή επικείμενες απειλές, συμπεριλαμβανομένων επιθέσεων ενάντια σε φορητές συσκευές, περιβάλλοντα υπολογιστικού νέφους και συσκευές του διαδικτύου των πραγμάτων.

Συμπληρωματικά προς την ανάλυση απειλών της CERT-ΕΕ, η Επιτροπή διενήργησε αξιολόγηση της λειτουργίας 20 θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης στον τομέα της κυβερνοασφάλειας. Από την αξιολόγηση αυτή αντλήθηκαν πληροφορίες σχετικά με τις καθιερωμένες πρακτικές κυβερνοασφάλειας και τις ικανότητες διαχείρισης της κυβερνοασφάλειας με εξωτερική συγκριτική αξιολόγηση ορισμένων τεχνικών ελέγχων ασφάλειας.

Η αξιολόγηση αυτή βασίστηκε σε ερωτηματολόγια στα οποία απάντησαν τα εν λόγω θεσμικά όργανα και οργανισμοί, δημοσίως διαθέσιμα δεδομένα και δεδομένα που παρασχέθηκαν απευθείας από τα ίδια τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Από την αξιολόγηση αντλήθηκαν επαρκείς πληροφορίες σχετικά με την τρέχουσα κατάσταση ώστε να συναχθούν τα εξής συμπεράσματα:

- Η ωριμότητα στον τομέα της κυβερνοασφάλειας, το μέγεθος των υποδομών ΤΠ και τα επίπεδα ικανότητας ποικίλλουν σημαντικά μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης που αξιολογήθηκαν.

[1] Ως «σημαντικό περιστατικό» νοείται κάθε περιστατικό του οποίου ο αντίκτυπος δεν είναι περιορισμένος και το οποίο είναι πιθανό να έχει ήδη κατανοηθεί πλήρως όσον αφορά τη μέθοδο ή τεχνολογία που χρησιμοποιήθηκε.

- Μολονότι πολλά θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης διαθέτουν ώριμες ικανότητες εντοπισμού και αντιμετώπισης εν γένει, παρατηρούνται διαφορές μεταξύ των επιπέδων ολοκληρωμένης διαχείρισης κινδύνων όσον αφορά τις οικείες ικανότητες διακυβέρνησης της κυβερνοασφάλειας.

- Ενώ γενικά τα πλαίσια κυβερνοασφάλειας (στρατηγική, πολιτική και βάση κανόνων) των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης που αξιολογήθηκαν είναι καλά εδραιωμένα στους βασικούς τομείς κυβερνοασφάλειας που απαριθμούνται στο παράρτημα Ι του κανονισμού, ορισμένα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης δεν διαθέτουν επαρκές επίπεδο ωριμότητας όσον αφορά τη διαχείριση της επιχειρησιακής συνέχειας, τη συμμόρφωση, τον έλεγχο και τη συνεχή βελτίωση.

- Διαπιστώθηκε ότι τα τεχνικά μέτρα που θεωρούνται βέλτιστες πρακτικές εφαρμόζονται ανομοιόμορφα από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που αξιολογήθηκαν.

Συνοπτικά, η ανάλυση των 20 θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης δείχνει ότι η διακυβέρνηση, η κυβερνοϋγιεινή, η συνολική ικανότητα και ωριμότητα ποικίλλουν σε ευρύ φάσμα. Ως εκ τούτου, η απαίτηση από όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης να εφαρμόζουν μια βασική δέσμη μέτρων κυβερνοασφάλειας είναι καθοριστικής σημασίας για την αντιμετώπιση αυτής της ανισότητας ως προς την ωριμότητα και για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας από όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

Μέχρι στιγμής καμία πράξη της ενωσιακής νομοθεσίας δεν αφορά ειδικά την κυβερνοασφάλεια των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης ούτε αντιμετωπίζει με ολοκληρωμένο τρόπο το τοπίο των απειλών κατά της κυβερνοασφάλειας και τους αναδυόμενους κινδύνους για την ΤΠ που προκύπτουν από την ψηφιοποίηση.

- **Διαβουλεύσεις με τα ενδιαφερόμενα μέρη**

Η Επιτροπή πραγματοποίησε διαβουλεύσεις με τα ενδιαφερόμενα μέρη σε όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και με εκπροσώπους των κρατών μελών στο Συμβούλιο και με ενδιαφερόμενα μέρη στο Ευρωπαϊκό Κοινοβούλιο. Στις 25 Ιουνίου 2021, εκπρόσωποι των κρατών μελών και των σχετικών ενδιαφερόμενων μερών από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης έλαβαν μέρος σε συνάντηση εργασίας που διοργάνωσε η Επιτροπή για να συζητήσουν το περιεχόμενο της μελλοντικής πρότασης κανονισμού.

- **Εκτίμηση επιπτώσεων**

Οι επιπτώσεις της παρούσας πρότασης θα αφορούν τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Αυτό καθιστά μη αναγκαία τη διενέργεια ειδικής εκτίμησης επιπτώσεων, καθώς δεν θα ισχύει για τα κράτη μέλη.

- **Θεμελιώδη δικαιώματα**

Η Ευρωπαϊκή Ένωση είναι προσηλωμένη στη διασφάλιση υψηλών προτύπων προστασίας των θεμελιωδών δικαιωμάτων. Κάθε ανταλλαγή πληροφοριών βάσει του παρόντος κανονισμού θα διεξάγεται σε περιβάλλοντα εμπιστοσύνης με πλήρη σεβασμό του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο

άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και στη σχετική νομοθεσία για την προστασία των δεδομένων, ιδίως στον κανονισμό (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

4. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Από δείκτες αναφοράς της αγοράς και μελέτες[2] προκύπτει ότι οι άμεσες δαπάνες για την κυβερνοασφάλεια τείνουν να κυμαίνονται μεταξύ 4 % και 7 % των συνολικών δαπανών των οργανισμών για την ΤΠ. Ωστόσο, η ανάλυση απειλών που διενήργησε η CERT-ΕΕ προς υποστήριξη της παρούσας νομοθετικής πρότασης δείχνει ότι διεθνείς φορείς και πολιτικοί οργανισμοί αντιμετωπίζουν αυξημένους κινδύνους και, ως εκ τούτου, ο στόχος βάσει του οποίου το 10 % των συνολικών δαπανών για την ΤΠ θα πρέπει να αφορά την κυβερνοασφάλεια φαίνεται καταλληλότερος. Το ακριβές κόστος των προσπαθειών αυτών δεν μπορεί να προσδιοριστεί λόγω της έλλειψης λεπτομερών στοιχείων σχετικά με τις δαπάνες των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης για την ΤΠ και το σχετικό ποσοστό των δαπανών για την κυβερνοασφάλεια.

Ως εκ τούτου, μολονότι είναι πιθανό πολλά θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης να δαπανούν λιγότερα για την κυβερνοασφάλεια απ' ό,τι θα έπρεπε, ο παρών κανονισμός δεν θα προκαλέσει από μόνος του αύξηση των εν λόγω τρεχουσών δαπανών. Ακόμη και χωρίς τον κανονισμό, κάθε οντότητα θα πρέπει να διασφαλίζει επαρκές επίπεδο κυβερνοασφάλειας. Ο κανονισμός αποτελεί συνέχεια της προηγούμενης συνεργασίας στο πλαίσιο της διοικούσας επιτροπής της CERT-ΕΕ και επισημοποιεί ένα επίπεδο ανταλλαγής πληροφοριών που σήμερα ήδη υπάρχει εν μέρει. Όπως περιγράφεται λεπτομερώς στο νομοθετικό δημοσιονομικό δελτίο, η CERT-ΕΕ θα απαιτήσει πρόσθετους πόρους για την εκπλήρωση του διευρυμένου ρόλου της και οι εν λόγω πόροι θα πρέπει να ανακατανεμηθούν από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που επωφελούνται από τις υπηρεσίες της CERT-ΕΕ.

5. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ

- **Εφαρμογή, ρυθμίσεις παρακολούθησης, αξιολόγησης και υποβολής εκθέσεων**

Το διοργανικό συμβούλιο κυβερνοασφάλειας (IICB), με τη συνδρομή της CERT-ΕΕ, θα πρέπει να επανεξετάσει τη λειτουργία του παρόντος κανονισμού, να διενεργήσει αξιολογήσεις και να υποβάλει έκθεση με τα πορίσματά του στην Επιτροπή. Η Επιτροπή θα πρέπει να διασφαλίζει την τακτική υποβολή εκθέσεων στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών.

Η CERT-ΕΕ δύναται να συντάσσει πρόταση για έγγραφο καθοδήγησης ή σύσταση, η θέσπιση του/της οποίου/-ας εναπόκειται στη διακριτική ευχέρεια του IICB. Το έγγραφο καθοδήγησης είναι συμβουλές που απευθύνονται στο σύνολο ή σε υποσύνολο των θεσμικών

[2] Πηγή: Gartner, «Identifying the Real Information Security Budget» (2016). Το κόστος αυτό προστίθεται στις έμμεσες δαπάνες για την ασφάλεια της ΤΠ, όπως είναι οι δαπάνες για την ασφάλεια των δικτύων, π.χ. τείχη προστασίας, προστασία από ιούς, και ευθύνες των ιδιοκτητών των συστημάτων, π.χ. αξιολόγηση κινδύνου και εφαρμογή ελέγχων ασφάλειας. Έγγραφο του 2020 ορίζει τις δαπάνες στον τομέα της κυβερνοασφάλειας στα χρηματοπιστωτικά ιδρύματα στο 10-11 % των δαπανών ΤΠ, πηγή: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

και λοιπών οργάνων και οργανισμών της Ένωσης, ενώ η σύσταση απευθύνεται σε μεμονωμένα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Η έκκληση για ανάληψη δράσης συνίσταται σε συμβουλές της CERT-ΕΕ που περιγράφουν επείγοντα μέτρα ασφάλειας τα οποία καλούνται να λάβουν τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης εντός καθορισμένου χρονικού πλαισίου.

- **Αναλυτική επεξήγηση των επιμέρους διατάξεων της πρότασης**

Γενικές διατάξεις

Ο κανονισμός θεσπίζει μέτρα που έχουν σκοπό να διασφαλίσουν υψηλό κοινό επίπεδο κυβερνοασφάλειας και εφαρμόζεται στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης ώστε να μπορούν να εκτελούν τις αντίστοιχες αποστολές τους με ανοικτό, αποτελεσματικό και ανεξάρτητο τρόπο. (άρθρα 1-3, 23-25)

Μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας

Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης υποχρεούνται να θεσπίσουν εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, το οποίο θα διασφαλίζει την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας. Επιπλέον, τα θεσμικά και λοιπά όργανα και οργανισμοί θεσπίζουν βασική δέσμη κανόνων κυβερνοασφάλειας για την αντιμετώπιση των κινδύνων που εντοπίζονται εντός του εν λόγω πλαισίου, διενεργούν σε τακτική βάση αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας και εγκρίνουν σχέδιο κυβερνοασφάλειας. (Άρθρα 4-8)

Διοργανικό συμβούλιο κυβερνοασφάλειας

Συστήνεται το διοργανικό συμβούλιο κυβερνοασφάλειας το οποίο είναι αρμόδιο για την παρακολούθηση της εφαρμογής του παρόντος κανονισμού από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και για την εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από τη CERT-ΕΕ και για την παροχή στρατηγικών κατευθύνσεων στη CERT-ΕΕ. (Άρθρα 9-11).

CERT-ΕΕ

Η CERT-ΕΕ συμβάλλει στην ασφάλεια του περιβάλλοντος ΤΠ όλων των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης παρέχοντάς τους συμβουλές, βοηθώντας τα να προλαμβάνουν, να εντοπίζουν, να μετριάζουν και να αντιμετωπίζουν περιστατικά και λειτουργώντας για αυτά ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας. (Άρθρα 12-17)

Υποχρεώσεις συνεργασίας και υποβολής εκθέσεων

Ο κανονισμός διασφαλίζει τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ της CERT-ΕΕ και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης με σκοπό την ανάπτυξη εμπιστοσύνης και αξιοπιστίας. Για τον σκοπό αυτό, η CERT-ΕΕ μπορεί να ζητεί από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης να της παρέχουν σχετικές πληροφορίες και να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης προκειμένου να διευκολύνεται ο εντοπισμός παρόμοιων κυβερνοαπειλών ή περιστατικών χωρίς τη συγκατάθεση του επηρεαζόμενου συνιστώντος οργάνου/οργανισμού. Η CERT-ΕΕ μπορεί να ανταλλάσσει

πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού κυβερνοασφάλειας μόνο με τη συγκατάθεση του επηρεαζόμενου συνιστώντος οργάνου/οργανισμού.

Ειδικότερα, όλα τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης κοινοποιούν στη CERT-ΕΕ σημαντικές κυβερνοαπειλές, σημαντικά τρωτά σημεία και σημαντικά περιστατικά χωρίς αδικαιολόγητη καθυστέρηση, και σε κάθε περίπτωση το αργότερο εντός 24 ωρών από τη στιγμή που λαμβάνουν γνώση αυτών. (Άρθρα 18-22)

2022/0085 (COD)

Πρόταση

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

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

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 298,

Έχοντας υπόψη τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενεργείας και ιδίως το άρθρο 106α,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Κατόπιν διαβίβασης του σχεδίου νομοθετικής πράξης στα εθνικά κοινοβούλια,

Αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία,

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, η τεχνολογία των πληροφοριών και των επικοινωνιών αποτελεί ακρογωνιαίο λίθο για μια ανοικτή, αποτελεσματική και ανεξάρτητη ενωσιακή διοίκηση. Η εξελισσόμενη τεχνολογία και η αυξημένη πολυπλοκότητα και διασυνδεσιμότητα των ψηφιακών συστημάτων επιτείνουν τους κινδύνους κυβερνοασφάλειας, καθιστώντας την ενωσιακή διοίκηση περισσότερο ευάλωτη σε κυβερνοαπειλές και σχετικά περιστατικά, στοιχείο που εντέλει απειλεί την επιχειρησιακή συνέχεια της διοίκησης και την ικανότητά της να προστατεύει τα δεδομένα της. Παρότι η αυξημένη χρήση των υπηρεσιών υπολογιστικού νέφους, η γενικευμένη χρήση της τεχνολογίας των πληροφοριών, ο υψηλός βαθμός ψηφιοποίησης, η τηλεργασία και η εξελισσόμενη τεχνολογία και συνδεσιμότητα αποτελούν σήμερα βασικά χαρακτηριστικά όλων των δραστηριοτήτων των διοικητικών οντοτήτων της Ένωσης, η ψηφιακή ανθεκτικότητα δεν έχει ακόμη αναπτυχθεί επαρκώς.

(2) Το τοπίο των κυβερνοαπειλών που αντιμετωπίζουν τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης εξελίσσεται συνεχώς. Οι τακτικές, οι τεχνικές και οι διαδικασίες που χρησιμοποιούνται από τους παράγοντες απειλής εξελίσσονται συνεχώς, ενώ τα κύρια κίνητρα για τέτοιες επιθέσεις μεταβάλλονται ελάχιστα, από την κλοπή πολύτιμων πληροφοριών που δεν έχουν δημοσιοποιηθεί έως τον προσπορισμό χρημάτων, τη χειραγώγηση της κοινής γνώμης ή την υπονόμευση των ψηφιακών υποδομών. Ο ρυθμός με τον οποίο πραγματοποιούν τις κυβερνοεπιθέσεις τους αυξάνεται συνεχώς, ενώ οι εκστρατείες τους γίνονται ολοένα και πιο εξελιγμένες

και αυτοματοποιημένες, στοχεύοντας σε επιφάνειες εκτεθειμένες σε επιθέσεις οι οποίες συνεχίζουν να επεκτείνονται, και εκμεταλλευόμενοι γρήγορα τα τρωτά σημεία.

(3) Τα περιβάλλοντα ΤΠ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης έχουν αλληλεξαρτήσεις και ενοποιημένες ροές δεδομένων, ενώ οι χρήστες τους συνεργάζονται στενά. Λόγω της διασύνδεσης αυτής, οποιαδήποτε διαταραχή, ακόμη και όταν αρχικά περιορίζεται σε συγκεκριμένο θεσμικό και λοιπό όργανο και οργανισμό της Ένωσης, μπορεί να επιφέρει ευρύτερα αλυσιδωτά αποτελέσματα και να έχει ενδεχομένως ως αποτέλεσμα εκτεταμένες και μακροχρόνιες αρνητικές επιπτώσεις σε άλλα όργανα ή οργανισμούς. Επιπλέον, τα περιβάλλοντα ΤΠ ορισμένων θεσμικών και λοιπών οργάνων και οργανισμών συνδέονται με τα περιβάλλοντα ΤΠ των κρατών μελών, με αποτέλεσμα ένα περιστατικό που επηρεάζει μία οντότητα της Ένωσης να ενέχει κίνδυνο για την κυβερνοασφάλεια των περιβαλλόντων ΤΠ των κρατών μελών και αντίστροφα.

(4) Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης αποτελούν ελκυστικούς στόχους και έρχονται αντιμέτωπα με παράγοντες απειλής οι οποίοι διαθέτουν υψηλή ειδίκευση και επάρκεια πόρων, καθώς και με άλλες απειλές. Ταυτόχρονα, το επίπεδο και η ωριμότητα της κυβερνοανθεκτικότητας, καθώς και η ικανότητα εντοπισμού και αντιμετώπισης κακόβουλων δραστηριοτήτων στον κυβερνοχώρο ποικίλλουν σημαντικά μεταξύ αυτών των οντοτήτων. Ως εκ τούτου, είναι αναγκαίο για τη λειτουργία της ευρωπαϊκής διοίκησης τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης να επιτύχουν υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω μιας βασικής δέσμης κανόνων κυβερνοασφάλειας (ενός συνόλου ελάχιστων κανόνων κυβερνοασφάλειας με τους οποίους πρέπει να συμμορφώνονται τα συστήματα δικτύου και πληροφοριών, καθώς και οι χειριστές και οι χρήστες τους, ώστε να ελαχιστοποιούνται οι κίνδυνοι κυβερνοασφάλειας), καθώς και μέσω ανταλλαγής πληροφοριών και συνεργασίας.

(5) Η οδηγία [πρόταση οδηγίας NIS 2] σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση αποσκοπεί στην περαιτέρω βελτίωση των ικανοτήτων ανθεκτικότητας και αντιμετώπισης περιστατικών στον τομέα της κυβερνοασφάλειας των δημόσιων και ιδιωτικών οντοτήτων, των εθνικών αρμόδιων αρχών και φορέων, καθώς και της Ένωσης στο σύνολό της. Επομένως, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης είναι ανάγκη να ακολουθήσουν παρόμοια πορεία θεσπίζοντας κανόνες που συμφωνούν με την οδηγία [πρόταση οδηγίας NIS 2] και αντικατοπτρίζουν το επίπεδο φιλοδοξίας της.

(6) Για να επιτευχθεί υψηλό κοινό επίπεδο κυβερνοασφάλειας, είναι αναγκαίο καθένα από τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης να θεσπίσει εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, το οποίο να διασφαλίζει την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας και να λαμβάνει υπόψη την επιχειρησιακή συνέχεια και τη διαχείριση κρίσεων.

(7) Οι διαφορές μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης απαιτούν ευελιξία κατά την εφαρμογή, δεδομένου ότι δεν ταιριάζει σε όλες τις περιπτώσεις η ίδια προσέγγιση. Τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας δεν θα πρέπει να περιλαμβάνουν υποχρεώσεις που παρεμβαίνουν άμεσα στην άσκηση των αποστολών που έχουν ανατεθεί στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης ή θίγουν τη θεσμική αυτονομία τους. Ως εκ τούτου, τα εν λόγω θεσμικά

και λοιπά όργανα και οργανισμοί θα πρέπει να θεσπίσουν τα δικά τους πλαίσια διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, και να εγκρίνουν τις δικές τους βασικές δέσμες κανόνων και τα δικά τους σχέδια κυβερνοασφάλειας.

(8) Για την αποφυγή δυσανάλογης οικονομικής και διοικητικής επιβάρυνσης των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, οι απαιτήσεις σχετικά με τη διαχείριση κινδύνων κυβερνοασφάλειας θα πρέπει να είναι ανάλογες προς τον κίνδυνο που ενέχει το σχετικό σύστημα δικτύου και πληροφοριών, λαμβανομένων υπόψη των πλέον προηγμένων τεχνολογικών εξελίξεων όσον αφορά τα σχετικά μέτρα. Κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης θα πρέπει να στοχεύει στη διάθεση επαρκούς ποσοστού του προϋπολογισμού του που αφορά την ΤΠ στη βελτίωση του επιπέδου κυβερνοασφάλειας. Μακροπρόθεσμα, θα πρέπει να επιδιωχθεί στόχος της τάξης του 10 %.

(9) Για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, η κυβερνοασφάλεια θα πρέπει να τελεί υπό την εποπτεία του ανώτατου διοικητικού επιπέδου κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης, όπου θα πρέπει να εγκριθεί βασική δέσμη κανόνων κυβερνοασφάλειας που θα πρέπει να αντιμετωπίζει τους κινδύνους που εντοπίζονται στο πλαίσιο που θα καθορισθεί από κάθε θεσμικό και λοιπό όργανο και οργανισμό. Η δημιουργία νοοτροπίας κυβερνοασφάλειας, δηλαδή η καθημερινή πρακτική της κυβερνοασφάλειας, αποτελεί αναπόσπαστο μέρος της βασικής δέσμης κανόνων κυβερνοασφάλειας σε όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

(10) Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα πρέπει να αξιολογούν τους κινδύνους που σχετίζονται με τις σχέσεις με τους προμηθευτές και τους παρόχους υπηρεσιών, συμπεριλαμβανομένων των παρόχων υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή υπηρεσιών διαχείρισης της ασφάλειας, και να λαμβάνουν κατάλληλα μέτρα για την αντιμετώπισή τους. Τα μέτρα αυτά θα πρέπει να αποτελούν μέρος της βασικής δέσμης κανόνων κυβερνοασφάλειας και να εξειδικεύονται περαιτέρω σε έγγραφα καθοδήγησης ή συστάσεις που εκδίδονται από τη CERT-ΕΕ. Κατά τον καθορισμό μέτρων και κατευθυντήριων γραμμών, θα πρέπει να λαμβάνονται δεόντως υπόψη η σχετική νομοθεσία και οι πολιτικές της ΕΕ, συμπεριλαμβανομένων των εκτιμήσεων κινδύνου και των συστάσεων που εκδίδονται από την ομάδα συνεργασίας NIS, όπως η συντονισμένη εκτίμηση κινδύνου της ΕΕ και η εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων πέμπτης γενιάς (5G). Επιπλέον, θα μπορούσε να απαιτείται πιστοποίηση των σχετικών προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ, στο πλαίσιο ειδικών συστημάτων πιστοποίησης της κυβερνοασφάλειας της ΕΕ που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881.

(11) Τον Μάιο του 2011, οι γενικοί γραμματείς των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης αποφάσισαν να συγκροτήσουν ομάδα προδιαμόρφωσης για την ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-ΕΕ), υπό την εποπτεία διοργανικής διοικούσας επιτροπής. Τον Ιούλιο του 2012, οι γενικοί γραμματείς επιβεβαίωσαν τις πρακτικές ρυθμίσεις και συμφώνησαν να διατηρηθεί η CERT-ΕΕ ως μόνιμη οντότητα ώστε να συνεχίσει να συμβάλλει στη βελτίωση του συνολικού επιπέδου ασφάλειας της τεχνολογίας πληροφοριών των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης ως παράδειγμα ορατής διοργανικής συνεργασίας στον

τομέα της κυβερνοασφάλειας. Τον Σεπτέμβριο του 2012, η CERT-ΕΕ συστάθηκε ως ειδική ομάδα της Ευρωπαϊκής Επιτροπής με διοργανική εντολή. Τον Δεκέμβριο του 2017, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης συνήψαν διοργανική ρύθμιση σχετικά με την οργάνωση και λειτουργία της CERT-ΕΕ[3]. Η εν λόγω ρύθμιση θα πρέπει να συνεχίσει να εξελίσσεται ώστε να στηρίζει την εφαρμογή του παρόντος κανονισμού.

(12) Η CERT-ΕΕ θα πρέπει να μετονομαστεί από «ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική» σε «Κέντρο Κυβερνοασφάλειας» για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, σύμφωνα με τις εξελίξεις στα κράτη μέλη και παγκοσμίως, όπου πολλές CERT μετονομάζονται σε κέντρα κυβερνοασφάλειας, αλλά θα πρέπει να διατηρήσει τη σύντομη ονομασία «CERT-ΕΕ» λόγω της αναγνώρισης της ονομασίας.

(13) Πολλές κυβερνοεπιθέσεις αποτελούν μέρος ευρύτερων εκστρατειών που έχουν ως στόχο ομάδες θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης ή κοινότητες ενδιαφέροντος που περιλαμβάνουν θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Για να καταστούν δυνατά ο προδραστικός εντοπισμός, η αντιμετώπιση περιστατικών ή η εφαρμογή μέτρων μετριασμού, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα πρέπει να κοινοποιούν στη CERT-ΕΕ σημαντικές κυβερνοαπειλές, σημαντικά τρωτά σημεία και σημαντικά περιστατικά και να ανταλλάσσουν κατάλληλες τεχνικές λεπτομέρειες που καθιστούν δυνατό τον εντοπισμό ή τον μετριασμό παρόμοιων κυβερνοαπειλών, τρωτών σημείων και περιστατικών, καθώς και την αντιμετώπισή τους, σε άλλα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Ακολουθώντας την ίδια προσέγγιση με αυτήν που προβλέπεται στην οδηγία [πρόταση οδηγίας NIS 2], όταν οι οντότητες λαμβάνουν γνώση σημαντικού περιστατικού, θα πρέπει να υποχρεούνται να υποβάλουν αρχική κοινοποίηση στη CERT-ΕΕ εντός 24 ωρών. Η εν λόγω ανταλλαγή πληροφοριών θα πρέπει να παρέχει στη CERT-ΕΕ τη δυνατότητα να διαδίδει τις πληροφορίες σε άλλα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και σε κατάλληλους ομολόγους τους, ώστε να συμβάλλει στην προστασία των περιβαλλόντων ΤΠ της Ένωσης και των περιβαλλόντων ΤΠ των ομολόγων της Ένωσης από παρόμοια περιστατικά, απειλές και τρωτά σημεία.

(14) Επιπλέον της ανάθεσης περισσότερων καθηκόντων και διευρυμένου ρόλου στη CERT-ΕΕ, θα πρέπει να δημιουργηθεί διοργανικό συμβούλιο κυβερνοασφάλειας (στο εξής: ΙΙCB), το οποίο θα πρέπει να διευκολύνει την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης μέσω της παρακολούθησης της εφαρμογής του παρόντος κανονισμού από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και μέσω της εποπτείας της υλοποίησης των γενικών προτεραιοτήτων και στόχων από τη CERT-ΕΕ και της παροχής στρατηγικών κατευθύνσεων στη CERT-ΕΕ. Το ΙΙCB θα πρέπει να διασφαλίζει την εκπροσώπηση των θεσμικών οργάνων και να περιλαμβάνει εκπροσώπους των λοιπών οργάνων και οργανισμών μέσω του Δικτύου Οργανισμών της Ένωσης.

(15) Η CERT-ΕΕ θα πρέπει να στηρίξει την εφαρμογή μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω προτάσεων για έγγραφα καθοδήγησης και συστάσεις προς το

[3] ΕΕ C 12 της 13.1.2018, σ. 1.

IICB ή μέσω της έκδοσης εκκλήσεων για ανάληψη δράσης. Τα εν λόγω έγγραφα καθοδήγησης και οι συστάσεις θα πρέπει να εγκρίνονται από το IICB. Όταν είναι απαραίτητο, η CERT-ΕΕ θα πρέπει να εκδίδει εκκλήσεις για ανάληψη δράσης στις οποίες περιγράφονται επείγοντα μέτρα ασφάλειας τα οποία καλούνται να λάβουν τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης εντός καθορισμένου χρονικού πλαισίου.

(16) Το IICB θα πρέπει να παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, καθώς και την παρακολούθηση των εγγράφων καθοδήγησης και των συστάσεων, και των εκκλήσεων για ανάληψη δράσης που εκδίδει η CERT-ΕΕ. Το IICB θα πρέπει να υποστηρίζεται σε τεχνικά θέματα από τεχνικές συμβουλευτικές ομάδες οι οποίες θα συγκροτούνται κατά την κρίση του IICB, οι οποίες θα πρέπει να συνεργάζονται στενά με τη CERT-ΕΕ, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και άλλα ενδιαφερόμενα μέρη, κατά περίπτωση. Όταν είναι αναγκαίο, το IICB θα πρέπει να εκδίδει μη δεσμευτικές προειδοποιήσεις και να προτείνει τη διενέργεια ελέγχων.

(17) Η CERT-ΕΕ θα πρέπει να έχει ως αποστολή να συμβάλλει στην ασφάλεια του περιβάλλοντος ΤΠ όλων των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Η CERT-ΕΕ θα πρέπει να λειτουργεί ως το αντίστοιχο όργανο του ορισθέντος συντονιστή για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, για τον σκοπό της συντονισμένης γνωστοποίησης τρωτών σημείων στο ευρωπαϊκό μητρώο τρωτών σημείων που αναφέρεται στο άρθρο 6 της οδηγίας [πρότασης οδηγίας NIS 2].

(18) Το 2020, η διοικούσα επιτροπή της CERT-ΕΕ έθεσε νέο στρατηγικό στόχο βάσει του οποίου η CERT-ΕΕ θα διασφαλίζει ολοκληρωμένο επίπεδο κυβερνοάμυνας για όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, το οποίο θα διαθέτει κατάλληλο εύρος και βάθος και θα προσαρμόζεται διαρκώς στις τρέχουσες ή επικείμενες απειλές, συμπεριλαμβανομένων επιθέσεων ενάντια σε φορητές συσκευές, περιβάλλοντα υπολογιστικού νέφους και συσκευές του διαδικτύου των πραγμάτων. Ο στρατηγικός στόχος θα περιλαμβάνει επίσης κέντρα επιχειρήσεων ασφάλειας (στο εξής: SOC) ευρέος φάσματος τα οποία θα επιτηρούν τα δίκτυα και θα εκτελούν παρακολούθηση 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα για τον εντοπισμό απειλών υψηλής σοβαρότητας. Όσον αφορά τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, η CERT-ΕΕ θα πρέπει να υποστηρίζει τις οικείες ομάδες ασφάλειας ΤΠ, μεταξύ άλλων μέσω παρακολούθησης πρώτης γραμμής 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα. Για τα μικρότερα και ορισμένα μεσαίου μεγέθους θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, η CERT-ΕΕ θα πρέπει να παρέχει όλες τις υπηρεσίες.

(19) Η CERT-ΕΕ θα πρέπει επίσης να εκπληρώνει τον ρόλο που προβλέπεται στην οδηγία [πρόταση οδηγίας NIS 2] όσον αφορά τη συνεργασία και την ανταλλαγή πληροφοριών με το δίκτυο των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT). Επιπλέον, σύμφωνα με τη σύσταση της Επιτροπής (ΕΕ) 2017/1584[4], η CERT-ΕΕ θα πρέπει να συνεργάζεται με τα σχετικά ενδιαφερόμενα μέρη και να συντονίζει από κοινού την αντιμετώπιση. Προκειμένου να συμβάλλει στην επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την

[4] Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

Ένωση, η CERT-ΕΕ θα πρέπει να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τους εθνικούς ομολόγους της. Η CERT-ΕΕ θα πρέπει επίσης να συνεργάζεται με άλλους ομολόγους από τον δημόσιο και τον ιδιωτικό τομέα, μεταξύ άλλων στο επίπεδο του ΝΑΤΟ, με την επιφύλαξη προηγούμενης έγκρισης από το ΙΙCB.

(20) Για τη στήριξη της επιχειρησιακής κυβερνοασφάλειας, η CERT-ΕΕ θα πρέπει να χρησιμοποιεί τη διαθέσιμη εμπειρογνωσία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια μέσω διαρθρωμένης συνεργασίας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5]. Όπου κρίνεται κατάλληλο, θα πρέπει να θεσπίζονται συγκεκριμένες ρυθμίσεις μεταξύ των δύο οντοτήτων με σκοπό τον καθορισμό της πρακτικής εφαρμογής της εν λόγω συνεργασίας και την αποφυγή της αλληλεπικάλυψης δραστηριοτήτων. Η CERT-ΕΕ θα πρέπει να συνεργάζεται με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια όσον αφορά την ανάλυση απειλών και να του κοινοποιεί την έκθεσή της για το τοπίο των απειλών σε τακτική βάση.

(21) Προς υποστήριξη της Κοινής Κυβερνομονάδας που δημιουργείται σύμφωνα με τη σύσταση της Επιτροπής της 23ης Ιουνίου 2021[6], η CERT-ΕΕ θα πρέπει να συνεργάζεται και να ανταλλάσσει πληροφορίες με τα ενδιαφερόμενα μέρη προκειμένου να προωθείται η επιχειρησιακή συνεργασία και να δίνεται στα υφιστάμενα δίκτυα η δυνατότητα να αξιοποιούν πλήρως τις δυνατότητές τους όσον αφορά την προστασία της Ένωσης.

(22) Σε όλες τις περιπτώσεις στις οποίες πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού, η επεξεργασία αυτή θα πρέπει να εκτελείται σύμφωνα με τη νομοθεσία για την προστασία των δεδομένων, συμπεριλαμβανομένου του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[7].

(23) Ο χειρισμός των πληροφοριών από τη CERT-ΕΕ και τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης θα πρέπει να συνάδει με τους κανόνες που ορίζονται στον κανονισμό [πρόταση κανονισμού για την ασφάλεια των πληροφοριών]. Για τη διασφάλιση συντονισμού σε ζητήματα ασφάλειας, κάθε επαφή με τη CERT-ΕΕ η οποία δρομολογείται ή επιδιώκεται από τις εθνικές υπηρεσίες ασφάλειας και πληροφοριών θα πρέπει να κοινοποιείται στη Διεύθυνση Ασφάλειας της Ευρωπαϊκής Επιτροπής και στον/στην πρόεδρο του ΙΙCB χωρίς αδικαιολόγητη καθυστέρηση.

---

5 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

6 Σύσταση C(2021) 4520 της Επιτροπής, της 23.6.2021, σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας.

7 Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

(24) Δεδομένου ότι οι υπηρεσίες και τα καθήκοντα της CERT-ΕΕ είναι προς το συμφέρον όλων των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης με δαπάνες ΤΠ θα πρέπει να συνεισφέρει δίκαιο μερίδιο στις εν λόγω υπηρεσίες και καθήκοντα. Οι συνεισφορές αυτές δεν θίγουν τη δημοσιονομική αυτονομία των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

(25) Το ΙΙCB, με τη συνδρομή της CERT-ΕΕ, θα πρέπει να επανεξετάζει και να αξιολογεί την εφαρμογή του παρόντος κανονισμού και να υποβάλει έκθεση με τα πορίσματά του στην Επιτροπή. Με βάση αυτά τα στοιχεία, η Επιτροπή θα πρέπει να υποβάλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών.

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Κεφάλαιο I
ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1
Αντικείμενο

Ο παρών κανονισμός θεσπίζει:

α) υποχρεώσεις βάσει των οποίων τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης οφείλουν να θεσπίσουν εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας·

β) υποχρεώσεις διαχείρισης κινδύνων κυβερνοασφάλειας και υποβολής εκθέσεων για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

γ) κανόνες σχετικά με την οργάνωση και τη λειτουργία του Κέντρου Κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (στο εξής: CERT-ΕΕ) και σχετικά με την οργάνωση και τη λειτουργία του διοργανικού συμβουλίου κυβερνοασφάλειας.

Άρθρο 2
Πεδίο εφαρμογής

Ο παρών κανονισμός εφαρμόζεται στη διαχείριση, διακυβέρνηση και έλεγχο κινδύνων κυβερνοασφάλειας από όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και στην οργάνωση και στη λειτουργία της CERT-ΕΕ και του διοργανικού συμβουλίου κυβερνοασφάλειας.

Άρθρο 3
Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης»: τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης που έχουν ιδρυθεί με τη Συνθήκη για την Ευρωπαϊκή Ένωση, τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης ή τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, ή βάσει των Συνθηκών αυτών·

2) «σύστημα δικτύου και πληροφοριών»: σύστημα δικτύου και πληροφοριών κατά την έννοια του άρθρου 4 σημείο 1) της οδηγίας [πρόταση οδηγίας NIS 2]·

3) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: ασφάλεια συστημάτων δικτύου και πληροφοριών κατά την έννοια του άρθρου 4 σημείο 2) της οδηγίας [πρόταση οδηγίας NIS 2]·

4) «κυβερνοασφάλεια»: κυβερνοασφάλεια κατά την έννοια του άρθρου 4 σημείο 3) της οδηγίας [πρόταση οδηγίας NIS 2]·

5) «ανώτατο διοικητικό επίπεδο»: διοικητικό στέλεχος, όργανο διοίκησης ή συντονισμού και εποπτείας στο ανώτερο διοικητικό επίπεδο, λαμβανομένων υπόψη των ρυθμίσεων διακυβέρνησης υψηλού επιπέδου σε κάθε θεσμικό και λοιπό όργανο και οργανισμό της Ένωσης·

6) «περιστατικό»: περιστατικό κατά την έννοια του άρθρου 4 σημείο 5) της οδηγίας [πρόταση οδηγίας NIS 2]·

7) «σημαντικό περιστατικό»: κάθε περιστατικό του οποίου ο αντίκτυπος δεν είναι περιορισμένος και το οποίο είναι πιθανό να έχει ήδη κατανοηθεί πλήρως όσον αφορά τη μέθοδο ή την τεχνολογία·

8) «σοβαρή επίθεση»: κάθε περιστατικό που απαιτεί περισσότερους πόρους από εκείνους που βρίσκονται στη διάθεση του επηρεαζόμενου θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης και της CERT-ΕΕ·

9) «χειρισμός περιστατικών»: χειρισμός περιστατικών κατά την έννοια του άρθρου 4 σημείο 6) της οδηγίας [πρόταση οδηγίας NIS 2]·

10) «κυβερνοαπειλή»: κυβερνοαπειλή κατά την έννοια του άρθρου 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881·

11) «σημαντική κυβερνοαπειλή»: κυβερνοαπειλή που πραγματοποιείται με την πρόθεση, την ευκαιρία και τη δυνατότητα πρόκλησης σημαντικού περιστατικού·

12) «τρωτό σημείο»: τρωτό σημείο κατά την έννοια του άρθρου 4 σημείο 8) της οδηγίας [πρόταση οδηγίας NIS 2]·

13) «σημαντικό τρωτό σημείο»: τρωτό σημείο που είναι πιθανό να οδηγήσει σε σημαντικό περιστατικό σε περίπτωση εκμετάλλευσής του·

14) «κίνδυνος κυβερνοασφάλειας»: κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με δυνητική δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών·

15) «Κοινή Κυβερνομονάδα»: εικονική και φυσική πλατφόρμα συνεργασίας για τις διάφορες κοινότητες κυβερνοασφάλειας στην Ένωση, με έμφαση στον

επιχειρησιακό και τεχνικό συντονισμό έναντι σοβαρών διασυνοριακών κυβερνοαπειλών και σχετικών περιστατικών κατά την έννοια της σύστασης της Επιτροπής, της 23ης Ιουνίου 2021·

16) «βασική δέσμη κανόνων κυβερνοασφάλειας»: σύνολο ελάχιστων κανόνων κυβερνοασφάλειας με τους οποίους πρέπει να συμμορφώνονται τα συστήματα δικτύου και πληροφοριών, καθώς και οι φορείς εκμετάλλευσης και οι χρήστες τους, ώστε να ελαχιστοποιούνται οι κίνδυνοι κυβερνοασφάλειας.

Κεφάλαιο ΙΙ
ΜΕΤΡΑ ΓΙΑ ΥΨΗΛΟ ΚΟΙΝΟ ΕΠΙΠΕΔΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 4
Διαχείριση, διακυβέρνηση και έλεγχος κινδύνων

1. Κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης θεσπίζει το δικό του εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας («το πλαίσιο») προς στήριξη της αποστολής της οντότητας και της άσκησης της θεσμικής αυτονομίας της. Το έργο αυτό εποπτεύεται από το ανώτατο διοικητικό επίπεδο της οντότητας, ώστε να διασφαλίζεται η αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας. Το πλαίσιο τίθεται σε εφαρμογή το αργότερο έως ….[15 μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού].

2. Το πλαίσιο καλύπτει ολόκληρο το περιβάλλον ΤΠ του οικείου θεσμικού ή λοιπού οργάνου ή οργανισμού, συμπεριλαμβανομένων τυχόν περιβάλλοντος ΤΠ εντός των εγκαταστάσεων, περιουσιακών στοιχείων και υπηρεσιών που λειτουργούν εξωτερικά σε περιβάλλοντα νεφοϋπολογιστικής ή φιλοξενούνται από τρίτους, κινητών συσκευών, εταιρικών δικτύων, επιχειρηματικών δικτύων που δεν συνδέονται με το διαδίκτυο και τυχόν συσκευών που συνδέονται με το περιβάλλον ΤΠ. Το πλαίσιο λαμβάνει υπόψη την επιχειρησιακή συνέχεια και τη διαχείριση κρίσεων και εξετάζει την ασφάλεια της εφοδιαστικής αλυσίδας, καθώς και τη διαχείριση ανθρώπινων κινδύνων που θα μπορούσαν να επηρεάσουν την κυβερνοασφάλεια του σχετικού θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης.

3. Το ανώτατο διοικητικό επίπεδο κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης εποπτεύει τη συμμόρφωση του οικείου οργάνου/οργανισμού με τις υποχρεώσεις που σχετίζονται με τη διαχείριση, τη διακυβέρνηση και τον έλεγχο κινδύνων κυβερνοασφάλειας, με την επιφύλαξη των επίσημων αρμοδιοτήτων άλλων επιπέδων διοίκησης για τη συμμόρφωση και τη διαχείριση κινδύνων στους αντίστοιχους τομείς αρμοδιότητάς τους.

4. Κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης εφαρμόζει αποτελεσματικούς μηχανισμούς για να διασφαλίζει ότι οι δαπάνες για την κυβερνοασφάλεια ανέρχονται σε επαρκές ποσοστό του προϋπολογισμού για την ΤΠ.

5. Κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης διορίζει τοπικό υπεύθυνο κυβερνοασφάλειας ή άλλο πρόσωπο με αντίστοιχες ευθύνες, που ενεργεί ως ενιαίο σημείο επαφής όσον αφορά όλες τις πτυχές της κυβερνοασφάλειας.

Άρθρο 5

Βασική δέσμη κανόνων κυβερνοασφάλειας

1. Το ανώτατο διοικητικό επίπεδο κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης εγκρίνει τη βασική δέσμη κανόνων κυβερνοασφάλειας της οντότητας για την αντιμετώπιση των κινδύνων που εντοπίζονται βάσει του πλαισίου που αναφέρεται στο άρθρο 4 παράγραφος 1. Το πράττει προς στήριξη της αποστολής της και της άσκησης της θεσμικής αυτονομίας της. Η βασική δέσμη κανόνων κυβερνοασφάλειας τίθεται σε εφαρμογή το αργότερο έως ....[18 μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού και καλύπτει τους τομείς που απαριθμούνται στο παράρτημα Ι και τα μέτρα που απαριθμούνται στο παράρτημα ΙΙ].

2. Τα ανώτερα διοικητικά στελέχη κάθε θεσμικού ή λοιπού οργάνου και οργανισμού της Ένωσης παρακολουθούν σε τακτική βάση ειδικά προγράμματα κατάρτισης, ώστε να αποκτούν επαρκείς γνώσεις και δεξιότητες προκειμένου να κατανοούν και να αξιολογούν τους κινδύνους και τις πρακτικές διαχείρισης της κυβερνοασφάλειας, καθώς και τον αντίκτυπό τους στις δραστηριότητες του οργανισμού.

Άρθρο 6

Αξιολογήσεις του επιπέδου ωριμότητας

Κάθε θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης διενεργεί αξιολόγηση του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας τουλάχιστον ανά τριετία, ενσωματώνοντας όλα τα στοιχεία του οικείου περιβάλλοντος ΤΠ, όπως περιγράφεται στο άρθρο 4, λαμβάνοντας υπόψη τα σχετικά έγγραφα καθοδήγησης και τις συστάσεις που εκδίδονται σύμφωνα με το άρθρο 13.

Άρθρο 7

Σχέδια κυβερνοασφάλειας

1. Σε συνέχεια των συμπερασμάτων που προκύπτουν από την αξιολόγηση του επιπέδου ωριμότητας και λαμβανομένων υπόψη των περιουσιακών στοιχείων και των κινδύνων που εντοπίζονται σύμφωνα με το άρθρο 4, το ανώτατο διοικητικό επίπεδο κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης εγκρίνει σχέδιο κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση έπειτα από τη θέσπιση του πλαισίου διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων και της βασικής δέσμης κανόνων κυβερνοασφάλειας. Το σχέδιο αποσκοπεί στην αύξηση της συνολικής κυβερνοασφάλειας της οικείας οντότητας και, ως εκ τούτου, συμβάλλει στην επίτευξη ή την ενίσχυση υψηλού κοινού επιπέδου κυβερνοασφάλειας μεταξύ όλων των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Προς στήριξη της αποστολής της οντότητας με βάση τη θεσμική της αυτονομία, το σχέδιο περιλαμβάνει τουλάχιστον τους τομείς που παρατίθενται στο παράρτημα Ι, τα μέτρα που παρατίθενται στο παράρτημα ΙΙ, καθώς και μέτρα που σχετίζονται με την ετοιμότητα, την αντιμετώπιση και την αποκατάσταση περιστατικών, όπως η παρακολούθηση της ασφάλειας και η καταγραφή. Το σχέδιο αναθεωρείται τουλάχιστον ανά τριετία, έπειτα από τις αξιολογήσεις του επιπέδου ωριμότητας που διενεργούνται σύμφωνα με το άρθρο 6.

2. Το σχέδιο κυβερνοασφάλειας περιλαμβάνει ρόλους και αρμοδιότητες των μελών του προσωπικού για την εφαρμογή του.

3. Το σχέδιο κυβερνοασφάλειας εξετάζει τυχόν εφαρμοστέα έγγραφα καθοδήγησης και συστάσεις που εκδίδονται από τη CERT-ΕΕ.

Άρθρο 8
Εφαρμογή

1. Αφού ολοκληρωθούν οι αξιολογήσεις του επιπέδου ωριμότητας, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης τις υποβάλλουν στο διοργανικό συμβούλιο κυβερνοασφάλειας. Αφού ολοκληρωθούν τα σχέδια ασφάλειας, τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης ενημερώνουν το διοργανικό συμβούλιο κυβερνοασφάλειας για την ολοκλήρωσή τους. Κατόπιν αιτήματος του συμβουλίου, υποβάλλουν εκθέσεις για συγκεκριμένες πτυχές του παρόντος κεφαλαίου.

2. Τα έγγραφα καθοδήγησης και οι συστάσεις, που εκδίδονται σύμφωνα με το άρθρο 13, υποστηρίζουν την εφαρμογή των διατάξεων του παρόντος κεφαλαίου.

Κεφάλαιο ΙΙΙ
ΔΙΟΡΓΑΝΙΚΟ ΣΥΜΒΟΥΛΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 9
Διοργανικό συμβούλιο κυβερνοασφάλειας

1. Ιδρύεται διοργανικό συμβούλιο κυβερνοασφάλειας (στο εξής: ΙΙCB).

2. Το ΙΙCB είναι αρμόδιο για:

α) την παρακολούθηση της εφαρμογής του παρόντος κανονισμού από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

β) την εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από τη CERT-ΕΕ και την παροχή στρατηγικών κατευθύνσεων στη CERT-ΕΕ.

3. Το ΙΙCB αποτελείται από τρεις εκπροσώπους τους οποίους διορίζει το Δίκτυο Οργανισμών της Ένωσης (στο εξής: EUAN) κατόπιν πρότασης της συμβουλευτικής επιτροπής ΤΠΕ (ICTAC) του εν λόγω Δικτύου για να εκπροσωπούν τα συμφέροντα των λοιπών οργάνων και οργανισμών που διαχειρίζονται το δικό τους περιβάλλον ΤΠ και από έναν εκπρόσωπο που ορίζει καθένα από τα κάτωθι όργανα:

α) το Ευρωπαϊκό Κοινοβούλιο,

β) το Συμβούλιο της Ευρωπαϊκής Ένωσης,

γ) η Ευρωπαϊκή Επιτροπή,

δ) το Δικαστήριο της Ευρωπαϊκής Ένωσης,

ε) η Ευρωπαϊκή Κεντρική Τράπεζα,

στ) το Ευρωπαϊκό Ελεγκτικό Συνέδριο,

ζ) η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης,

η) η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή,

θ) η Ευρωπαϊκή Επιτροπή των Περιφερειών,

ι) η Ευρωπαϊκή Τράπεζα Επενδύσεων,

ια) ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια.

Τα μέλη μπορούν να επικουρούνται από αναπληρωτή. Ο/Η πρόεδρος μπορεί να προσκαλεί και άλλους εκπροσώπους των οργανισμών που απαριθμούνται ανωτέρω ή άλλων θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης να παραστούν στις συνεδριάσεις του IICB χωρίς δικαίωμα ψήφου.

4. Το IICB θεσπίζει τον εσωτερικό κανονισμό του.

5. Το IICB ορίζει πρόεδρο, σύμφωνα με τον εσωτερικό κανονισμό του, μεταξύ των μελών του για τετραετή θητεία. Το πρόσωπο που τον/την αναπληρώνει καθίσταται τακτικό μέλος του IICB για την ίδια θητεία.

6. Το IICB συνεδριάζει με πρωτοβουλία του/της προέδρου του, κατόπιν αιτήματος της CERT-EE ή κατόπιν αιτήματος οποιουδήποτε από τα μέλη του.

7. Κάθε μέλος του IICB διαθέτει μία ψήφο. Οι αποφάσεις του IICB λαμβάνονται με απλή πλειοψηφία, εκτός εάν προβλέπεται διαφορετικά στον παρόντα κανονισμό. Ο/Η πρόεδρος δεν ψηφίζει παρά μόνο σε περίπτωση ισοψηφίας, οπότε υπερισχύει η δική του/της ψήφος.

8. Το IICB μπορεί να ενεργεί με απλουστευμένη γραπτή διαδικασία που κινείται σύμφωνα με τον εσωτερικό κανονισμό του IICB. Σύμφωνα με τη διαδικασία αυτή, η σχετική απόφαση θεωρείται εγκριθείσα εντός της προθεσμίας που ορίζει ο/η πρόεδρος, εκτός εάν ένα μέλος διατυπώσει αντιρρήσεις.

9. Ο/Η επικεφαλής της CERT-EE, ή ο αναπληρωτής / η αναπληρώτριά του/της, συμμετέχει στις συνεδριάσεις του IICB, εκτός εάν το IICB αποφασίσει διαφορετικά.

10. Η Επιτροπή παρέχει γραμματειακή υποστήριξη στο IICB.

11. Οι εκπρόσωποι που ορίζονται από το EUAN κατόπιν πρότασης της συμβουλευτικής επιτροπής ΤΠΕ διαβιβάζουν τις αποφάσεις του IICB στους οργανισμούς και στις κοινές επιχειρήσεις της Ένωσης. Κάθε οργανισμός ή λοιπό όργανο της Ένωσης έχει το δικαίωμα να επιστήσει την προσοχή των εκπροσώπων ή του/της προέδρου του IICB σε οποιοδήποτε ζήτημα θεωρεί ότι πρέπει να τεθεί υπόψη του IICB.

12. Το IICB δύναται να αναλάβει δράση με απλουστευμένη γραπτή διαδικασία από τον/την πρόεδρο, βάσει του οποίου η σχετική απόφαση θεωρείται εγκριθείσα εντός της προθεσμίας που ορίζει ο/η πρόεδρος, εκτός εάν κάποιο μέλος διατυπώσει αντιρρήσεις.

13. Το ΙΙCB μπορεί να διορίσει εκτελεστική επιτροπή για να το επικουρεί στο έργο του και να της αναθέσει ορισμένα από τα καθήκοντα και τις αρμοδιότητές του. Το ΙΙCB θεσπίζει τον κανονισμό της εκτελεστικής επιτροπής, συμπεριλαμβανομένων των καθηκόντων και εξουσιών της και της θητείας των μελών της.

Άρθρο 10
Καθήκοντα του ΙΙCB

Κατά την άσκηση των αρμοδιοτήτων του, το ΙΙCB ειδικότερα:

α) εξετάζει τυχόν εκθέσεις που ζητούνται από τη CERT-ΕΕ σχετικά με την κατάσταση εφαρμογής του παρόντος κανονισμού από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

β) εγκρίνει, βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ, το ετήσιο πρόγραμμα εργασιών της CERT-ΕΕ και παρακολουθεί την εφαρμογή του·

γ) εγκρίνει, βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ, τον κατάλογο υπηρεσιών της CERT-ΕΕ·

δ) εγκρίνει, βάσει πρότασης που υποβάλλει ο/ή επικεφαλής της CERT-ΕΕ, τον ετήσιο οικονομικό προγραμματισμό των εσόδων και των εξόδων, συμπεριλαμβανομένης της στελέχωσης, για τις δραστηριότητες της CERT-ΕΕ·

ε) εγκρίνει, βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ, τις λεπτομέρειες για τις συμφωνίες επιπέδου υπηρεσιών·

στ) εξετάζει και εγκρίνει την ετήσια έκθεση που καταρτίζει ο/η επικεφαλής της CERT-ΕΕ, η οποία καλύπτει τις δραστηριότητες της CERT-ΕΕ και την από μέρους της διαχείριση κονδυλίων·

ζ) εγκρίνει και παρακολουθεί τους βασικούς δείκτες επιδόσεων της CERT-ΕΕ, οι οποίοι καθορίζονται βάσει πρότασης του/της επικεφαλής της CERT-ΕΕ·

η) εγκρίνει ρυθμίσεις συνεργασίας, ρυθμίσεις ή συμβάσεις επιπέδου υπηρεσιών μεταξύ της CERT-ΕΕ και άλλων οντοτήτων σύμφωνα με το άρθρο 17·

θ) συγκροτεί όσες τεχνικές συμβουλευτικές ομάδες απαιτούνται για να συνδράμουν το ΙΙCB στο έργο του, εγκρίνει την εντολή τους και ορίζει τον/την πρόεδρο κάθε ομάδας.

Άρθρο 11
Συμμόρφωση

Το ΙΙCB παρακολουθεί την εφαρμογή του παρόντος κανονισμού και των εκδοθέντων εγγράφων καθοδήγησης, συστάσεων και εκκλήσεων για ανάληψη δράσης από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Όταν το ΙΙCB διαπιστώσει ότι θεσμικά και λοιπά όργανα και οργανισμοί δεν έχουν εφαρμόσει ή υλοποιήσει με αποτελεσματικό τρόπο τον παρόντα κανονισμό ή έγγραφα καθοδήγησης, συστάσεις και εκκλήσεις για ανάληψη δράσης

που έχουν εκδοθεί δυνάμει του παρόντος κανονισμού, με την επιφύλαξη των εσωτερικών διαδικασιών του οικείου θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης, δύναται:

α) να εκδώσει προειδοποίηση· όταν είναι αναγκαίο λόγω επιτακτικού κινδύνου κυβερνοασφάλειας, ο αποδέκτης της προειδοποίησης περιορίζεται καταλλήλως·

β) να συστήσει σε αρμόδια υπηρεσία ελέγχου να διενεργήσει έλεγχο.

Κεφάλαιο IV
CERT-ΕΕ

Άρθρο 12
Αποστολή και καθήκοντα της CERT-ΕΕ

1. Αποστολή της CERT-ΕΕ, του αυτόνομου διοργανικού Κέντρου Κυβερνοασφάλειας για όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης είναι να συμβάλλει στην ασφάλεια του μη διαβαθμισμένου περιβάλλοντος ΤΠ όλων των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, παρέχοντάς τους συμβουλές σχετικά με την κυβερνοασφάλεια, βοηθώντας τους στην πρόληψη, στον εντοπισμό, στον μετριασμό και στην αντιμετώπιση περιστατικών και λειτουργώντας για αυτά ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας.

2. Η CERT-ΕΕ εκτελεί τα ακόλουθα καθήκοντα για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης:

   α) τα στηρίζει κατά την εφαρμογή του παρόντος κανονισμού και συμβάλλει στον συντονισμό της εφαρμογής του παρόντος κανονισμού μέσω των μέτρων που παρατίθενται στο άρθρο 13 παράγραφος 1 ή μέσω ad-hoc εκθέσεων τις οποίες ζητά το ΙΙCB·

   β) τα στηρίζει με μια δέσμη υπηρεσιών κυβερνοασφάλειας που περιγράφονται στον κατάλογο υπηρεσιών της (στο εξής: βασικές υπηρεσίες)·

   γ) διατηρεί δίκτυο ομοτίμων και εταίρων για τη στήριξη των υπηρεσιών που περιγράφονται στα άρθρα 16 και 17·

   δ) εφιστά την προσοχή του ΙΙCB σε κάθε ζήτημα που αφορά την εφαρμογή του παρόντος κανονισμού και την εφαρμογή των εγγράφων καθοδήγησης, των συστάσεων και των εκκλήσεων για ανάληψη δράσης·

   ε) υποβάλλει εκθέσεις σχετικά με τις κυβερνοαπειλές που αντιμετωπίζουν τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης και συμβάλλει στην επίγνωση της κατάστασης στον κυβερνοχώρο στην ΕΕ.

3. Η CERT-ΕΕ συνεισφέρει στην Κοινή Κυβερνομονάδα που δημιουργείται σύμφωνα με τη σύσταση της Επιτροπής της 23ης Ιουνίου 2021, μεταξύ άλλων στους ακόλουθους τομείς:

α) ετοιμότητα, συντονισμός σε περίπτωση περιστατικών, ανταλλαγή πληροφοριών και αντιμετώπιση κρίσεων σε τεχνικό επίπεδο σε περιπτώσεις που συνδέονται με θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης·

β) επιχειρησιακή συνεργασία όσον αφορά το δίκτυο ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT), μεταξύ άλλων όσον αφορά την αμοιβαία συνδρομή, και την ευρύτερη κοινότητα κυβερνοασφάλειας·

γ) πληροφορίες για κυβερνοαπειλές, συμπεριλαμβανομένης της επίγνωσης της κατάστασης·

δ) για κάθε θέμα για το οποίο είναι απαραίτητη η τεχνική εμπειρογνωσία της CERT-ΕΕ στον τομέα της κυβερνοασφάλειας.

4. Η CERT-ΕΕ συμμετέχει σε διαρθρωμένη συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια όσον αφορά την ανάπτυξη ικανοτήτων, την επιχειρησιακή συνεργασία και τις μακροπρόθεσμες στρατηγικές αναλύσεις των κυβερνοαπειλών σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

5. Η CERT-ΕΕ μπορεί να παρέχει τις κάτωθι υπηρεσίες που δεν περιγράφονται στον κατάλογο υπηρεσιών της (στο εξής: χρεώσιμες υπηρεσίες):

α) υπηρεσίες που υποστηρίζουν την κυβερνοασφάλεια του περιβάλλοντος ΤΠ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 2, βάσει συμφωνιών επιπέδου υπηρεσιών και υπό την προϋπόθεση ότι υπάρχουν οι διαθέσιμοι πόροι·

β) υπηρεσίες που υποστηρίζουν δραστηριότητες ή έργα των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης στον τομέα της κυβερνοασφάλειας, πέραν αυτών που αποσκοπούν στην προστασία του περιβάλλοντος ΤΠ των οργάνων αυτών, βάσει γραπτών συμφωνιών και με την προηγούμενη έγκριση του ΙΙCB·

γ) υπηρεσίες που υποστηρίζουν την ασφάλεια του περιβάλλοντος ΤΠ σε οργανισμούς άλλους πέραν των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης που συνεργάζονται στενά με θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, για παράδειγμα με την ανάθεση καθηκόντων ή αρμοδιοτήτων δυνάμει του ενωσιακού δικαίου, βάσει γραπτών συμφωνιών και με την προηγουμένη έγκριση του ΙΙCB.

6. Η CERT-ΕΕ μπορεί να διοργανώνει ασκήσεις κυβερνοασφάλειας ή να συστήνει τη συμμετοχή σε υφιστάμενες ασκήσεις, σε στενή συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, κατά περίπτωση, με σκοπό τη δοκιμή του επιπέδου κυβερνοασφάλειας των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

7. Η CERT-ΕΕ μπορεί να παρέχει συνδρομή σε θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης όσον αφορά περιστατικά σε διαβαθμισμένα περιβάλλοντα ΤΠ, κατόπιν σχετικού ρητού αιτήματος από το οικείο συνιστών όργανο.

Άρθρο 13

Έγγραφα καθοδήγησης, συστάσεις και εκκλήσεις για ανάληψη δράσης

1. Η CERT-ΕΕ υποστηρίζει την εφαρμογή του παρόντος κανονισμού εκδίδοντας:

   α) εκκλήσεις για ανάληψη δράσης που περιγράφουν επείγοντα μέτρα ασφάλειας τα οποία καλούνται να λάβουν τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης εντός καθορισμένου χρονικού πλαισίου·

   β) προτάσεις προς το ΙΙCB για έγγραφα καθοδήγησης που απευθύνονται σε όλα ή σε υποσύνολο των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης·

   γ) προτάσεις προς το ΙΙCB για συστάσεις που απευθύνονται σε μεμονωμένα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

2. Τα έγγραφα καθοδήγησης και οι συστάσεις μπορούν να περιλαμβάνουν:

   α) λεπτομέρειες ή βελτιώσεις για τη διαχείριση κινδύνων κυβερνοασφάλειας και τη βασική δέσμη κανόνων κυβερνοασφάλειας·

   β) λεπτομέρειες για τις αξιολογήσεις του επιπέδου ωριμότητας και τα σχέδια κυβερνοασφάλειας· και

   γ) κατά περίπτωση, τη χρήση κοινής τεχνολογίας, κοινής αρχιτεκτονικής και κοινών συναφών βέλτιστων πρακτικών με στόχο την επίτευξη διαλειτουργικότητας και κοινών προτύπων κατά την έννοια του άρθρου 4 παράγραφος 10 της οδηγίας [πρόταση οδηγίας NIS 2].

3. Το ΙΙCB δύναται να εκδίδει έγγραφα καθοδήγησης ή συστάσεις κατόπιν πρότασης της CERT-ΕΕ.

4. Το ΙΙCB δύναται να εκδίδει εντολή προς τη CERT-ΕΕ για την έκδοση, την ανάκληση ή την τροποποίηση πρότασης για έγγραφα καθοδήγησης ή συστάσεις ή ανάληψη δράσης.

Άρθρο 14

Επικεφαλής της CERT-ΕΕ

Ο/Η επικεφαλής της CERT-ΕΕ υποβάλλει τακτικά εκθέσεις στο ΙΙCB και στον/στην πρόεδρο του ΙΙCB σχετικά με τις επιδόσεις της CERT-ΕΕ, τον οικονομικό σχεδιασμό, τα έσοδα, την εκτέλεση του προϋπολογισμού, τις συμφωνίες επιπέδου υπηρεσιών και τις γραπτές συμφωνίες που έχουν συναφθεί, τη συνεργασία με ομολόγους και εταίρους, καθώς και σχετικά με τις αποστολές που αναλαμβάνει το προσωπικό, συμπεριλαμβανομένων των εκθέσεων που αναφέρονται στο άρθρο 10 παράγραφος 1.

Άρθρο 15

Οικονομικά θέματα και θέματα προσωπικού

1. Η Επιτροπή, αφού λάβει την ομόφωνη έγκριση του ΙΙCB, διορίζει τον/την επικεφαλής της CERT-ΕΕ. Ζητείται η γνώμη του ΙΙCB σε όλα τα στάδια της

διαδικασίας πριν από τον διορισμό του/της επικεφαλής της CERT-ΕΕ, ειδικότερα για τη σύνταξη προκηρύξεων κενής θέσης, την εξέταση των αιτήσεων και τον ορισμό των εξεταστικών επιτροπών σε σχέση με την εκάστοτε θέση.

2. Για την εφαρμογή των διοικητικών και δημοσιονομικών διαδικασιών, ο/η επικεφαλής της CERT-ΕΕ ενεργεί υπό τον έλεγχο της Επιτροπής.

3. Τα καθήκοντα και οι δραστηριότητες της CERT-ΕΕ, συμπεριλαμβανομένων των υπηρεσιών που παρέχονται από τη CERT-ΕΕ σύμφωνα με το άρθρο 12 παράγραφοι 2, 3, 4 και 6 και το άρθρο 13 παράγραφος 1 στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης τα οποία χρηματοδοτούνται από τον τομέα του πολυετούς δημοσιονομικού πλαισίου που είναι αφιερωμένος στην ευρωπαϊκή δημόσια διοίκηση, χρηματοδοτούνται μέσω χωριστής γραμμής του προϋπολογισμού της Επιτροπής. Οι ειδικές θέσεις της CERT-ΕΕ περιγράφονται λεπτομερώς σε υποσημείωση του πίνακα προσωπικού της Επιτροπής.

4. Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 3, καταβάλλουν ετήσια χρηματοδοτική συνεισφορά στη CERT-ΕΕ για την κάλυψη των υπηρεσιών που παρέχει η CERT-ΕΕ σύμφωνα με την εν λόγω παράγραφο 3. Οι αντίστοιχες συνεισφορές βασίζονται σε κατευθύνσεις που παρέχει το IICB και συμφωνούνται μεταξύ της κάθε οντότητας και της CERT-ΕΕ στο πλαίσιο συμφωνιών επιπέδου υπηρεσιών. Οι συνεισφορές αντιστοιχούν σε δίκαιο και αναλογικό ποσοστό του συνολικού κόστους των παρεχόμενων υπηρεσιών. Εισπράττονται από τη χωριστή γραμμή του προϋπολογισμού που αναφέρεται στην παράγραφο 3 ως έσοδα για ειδικό προορισμό, όπως προβλέπεται στο άρθρο 21 παράγραφος 3 στοιχείο γ) του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[8].

5. Οι δαπάνες για τα καθήκοντα που ορίζονται στο άρθρο 12 παράγραφος 5 ανακτώνται από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που λαμβάνουν τις υπηρεσίες της CERT-ΕΕ. Τα έσοδα εγγράφονται στις γραμμές του προϋπολογισμού που καλύπτουν τις δαπάνες.

Άρθρο 16

Συνεργασία της CERT-ΕΕ με τους ομολόγους της από κράτη μέλη

1. Η CERT-ΕΕ συνεργάζεται και ανταλλάσσει πληροφορίες με εθνικούς ομολόγους στα κράτη μέλη, συμπεριλαμβανομένων των ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), των εθνικών Κέντρων Κυβερνοασφάλειας, των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) και των ενιαίων σημείων επαφής που αναφέρονται στο άρθρο 8 της οδηγίας [πρόταση οδηγίας NIS 2], σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά, καθώς και σχετικά με πιθανά αντίμετρα και όλα τα θέματα που αφορούν τη βελτίωση της

[8] Κανονισμός (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 (ΕΕ L 193 της 30.7.2018, σ. 1).

προστασίας των περιβαλλόντων ΤΠ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, μεταξύ άλλων μέσω του δικτύου CSIRT που αναφέρεται στο άρθρο 13 της οδηγίας [πρόταση οδηγίας NIS 2].

2. Η CERT-ΕΕ μπορεί να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τους εθνικούς ομολόγους στα κράτη μέλη προκειμένου να διευκολύνεται ο εντοπισμός παρόμοιων κυβερνοαπειλών ή περιστατικών χωρίς τη συγκατάθεση του επηρεαζόμενου συνιστώντος οργάνου/οργανισμού. Η CERT-ΕΕ μπορεί να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού κυβερνοασφάλειας μόνο με τη συγκατάθεση του επηρεαζόμενου συνιστώντος οργάνου/οργανισμού.

Άρθρο 17

Συνεργασία της CERT-ΕΕ με τους ομολόγους της από τρίτες χώρες

1. Η CERT-ΕΕ μπορεί να συνεργάζεται με ομολόγους της από τρίτες χώρες, συμπεριλαμβανομένων ομολόγων ανά κλάδο, σχετικά με εργαλεία και μεθόδους, όπως τεχνικές, τακτικές, διαδικασίες και βέλτιστες πρακτικές, καθώς και σχετικά με κυβερνοαπειλές και τρωτά σημεία. Για κάθε συνεργασία με τους εν λόγω ομολόγους, μεταξύ άλλων σε πλαίσια όπου οι ομόλογοι από τρίτες χώρες συνεργάζονται με εθνικούς ομολόγους των κρατών μελών, η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΙΙCB.

2. Η CERT-ΕΕ μπορεί να συνεργάζεται με άλλους εταίρους, όπως εμπορικές οντότητες, διεθνείς οργανισμούς, εθνικές οντότητες εκτός Ευρωπαϊκής Ένωσης ή μεμονωμένους εμπειρογνώμονες, για τη συλλογή πληροφοριών σχετικά με γενικές και ειδικές κυβερνοαπειλές, γενικά και ειδικά τρωτά σημεία, και γενικά και ειδικά πιθανά αντίμετρα. Για ευρύτερη συνεργασία με τους εταίρους αυτούς, η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΙΙCB.

3. Η CERT-ΕΕ μπορεί, με τη συγκατάθεση του επηρεαζόμενου από περιστατικό συνιστώντος οργάνου/οργανισμού, να παρέχει πληροφορίες σχετικά με το περιστατικό στους εταίρους που μπορούν να συμβάλλουν στην ανάλυση του περιστατικού.

Κεφάλαιο V
ΥΠΟΧΡΕΩΣΕΙΣ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΥΠΟΒΟΛΗΣ ΕΚΘΕΣΕΩΝ

Άρθρο 18

Χειρισμός πληροφοριών

1. Η CERT-ΕΕ και τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης τηρούν την υποχρέωση τήρησης του επαγγελματικού απορρήτου σύμφωνα με το άρθρο 339 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης ή ισοδύναμα εφαρμοστέα πλαίσια.

2. Οι διατάξεις του κανονισμού (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[9] εφαρμόζονται όσον αφορά αιτήματα πρόσβασης του κοινού σε έγγραφα που βρίσκονται στην κατοχή της CERT-ΕΕ, λαμβανομένης υπόψη της υποχρέωσης που απορρέει από τον εν λόγω κανονισμό για διαβούλευση με άλλα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης όταν το αίτημα αφορά τα έγγραφά τους.

3. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει του παρόντος κανονισμού υπόκειται στον κανονισμό (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

4. Ο χειρισμός πληροφοριών από τη CERT-ΕΕ και τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ συνάδει με τους κανόνες που θεσπίζονται στην [πρόταση κανονισμού για την ασφάλεια των πληροφοριών].

5. Κάθε επαφή με τη CERT-ΕΕ η οποία δρομολογείται ή επιδιώκεται από τις εθνικές υπηρεσίες ασφάλειας και πληροφοριών κοινοποιείται στη Διεύθυνση Ασφάλειας της Επιτροπής και στον/στην πρόεδρο του IICB χωρίς αδικαιολόγητη καθυστέρηση.

Άρθρο 19
Υποχρεώσεις ανταλλαγής

1. Για να είναι η CERT-ΕΕ σε θέση να συντονίζει τη διαχείριση τρωτών σημείων και την αντιμετώπιση περιστατικών, μπορεί να ζητεί από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης να της παρέχουν πληροφορίες από τις αντίστοιχες απογραφές των οικείων συστημάτων ΤΠ οι οποίες είναι σημαντικές για τη στήριξη της CERT-ΕΕ. Το θεσμικό και λοιπό όργανο και οργανισμός στο οποίο υποβάλλεται το αίτημα διαβιβάζει τις ζητούμενες πληροφορίες, καθώς και τυχόν μεταγενέστερες επικαιροποιήσεις τους, χωρίς αδικαιολόγητη καθυστέρηση.

2. Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης, κατόπιν αιτήματος της CERT-ΕΕ και χωρίς αδικαιολόγητη καθυστέρηση, της παρέχουν ψηφιακές πληροφορίες που δημιουργούνται από τη χρήση ηλεκτρονικών συσκευών που εμπλέκονται στα αντίστοιχα περιστατικά τους. Η CERT-ΕΕ μπορεί να διευκρινίζει περαιτέρω ποια είναι τα απαιτούμενα από αυτή είδη των εν λόγω ψηφιακών πληροφοριών με σκοπό την επίγνωση της κατάστασης και την αντιμετώπιση περιστατικών.

3. Η CERT-ΕΕ μπορεί να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του επηρεαζόμενου από το περιστατικό θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης μόνο με τη συγκατάθεση της εν λόγω οντότητας. Η CERT-ΕΕ μπορεί να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού κυβερνοασφάλειας μόνο με τη συγκατάθεση της επηρεαζόμενης από το περιστατικό οντότητας.

[9] Κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (ΕΕ L 145 της 31.5.2001, σ. 43).

4. Οι υποχρεώσεις ανταλλαγής δεν επεκτείνονται στις διαβαθμισμένες πληροφορίες ΕΕ (στο εξής: ΔΠΕΕ) και στις πληροφορίες που έχει λάβει θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης από υπηρεσία ασφάλειας ή πληροφοριών ή υπηρεσία επιβολής του νόμου κράτους μέλους υπό τη ρητή προϋπόθεση ότι δεν θα κοινοποιηθούν στη CERT-ΕΕ.

Άρθρο 20
Υποχρεώσεις κοινοποίησης

1. Όλα τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης προβαίνουν σε αρχική κοινοποίηση σημαντικών κυβερνοαπειλών, σημαντικών τρωτών σημείων και σημαντικών περιστατικών στη CERT-ΕΕ, χωρίς αδικαιολόγητη καθυστέρηση, και σε κάθε περίπτωση το αργότερο εντός 24 ωρών από τη στιγμή που λαμβάνουν γνώση τους.

   Σε δεόντως αιτιολογημένες περιπτώσεις και σε συμφωνία με τη CERT-ΕΕ, το οικείο θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης δύναται να παρεκκλίνει από την προθεσμία που ορίζεται στην προηγούμενη παράγραφο.

2. Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης κοινοποιούν περαιτέρω στη CERT-ΕΕ, χωρίς αδικαιολόγητη καθυστέρηση, κατάλληλες τεχνικές λεπτομέρειες σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά που καθιστούν δυνατό τον εντοπισμό, την αντιμετώπιση περιστατικών ή τη λήψη μέτρων μετριασμού. Η κοινοποίηση περιλαμβάνει τα κάτωθι στοιχεία, εφόσον είναι διαθέσιμα:

   α) τους σχετικούς δείκτες έκθεσης σε κίνδυνο·

   β) τους σχετικούς μηχανισμούς εντοπισμού·

   γ) τις δυνητικές επιπτώσεις·

   δ) τα σχετικά μέτρα μετριασμού.

3. Η CERT-ΕΕ υποβάλλει στον ENISA σε μηνιαία βάση συνοπτική έκθεση που περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με σημαντικές κυβερνοαπειλές, σημαντικά τρωτά σημεία και σημαντικά περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 1.

4. Το ΙΙCB μπορεί να εκδίδει έγγραφα καθοδήγησης ή συστάσεις σχετικά με τις λεπτομέρειες και το περιεχόμενο της κοινοποίησης. Η CERT-ΕΕ διαδίδει τις κατάλληλες τεχνικές λεπτομέρειες ώστε να διευκολύνει τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης στον προδραστικό εντοπισμό, στην αντιμετώπιση περιστατικών ή στην εφαρμογή μέτρων μετριασμού.

5. Οι υποχρεώσεις κοινοποίησης δεν επεκτείνονται στις ΔΠΕΕ και στις πληροφορίες που έχει λάβει θεσμικό και λοιπό όργανο και οργανισμός της Ένωσης από υπηρεσία ασφάλειας ή πληροφοριών ή υπηρεσία επιβολής του νόμου κράτους μέλους υπό τη ρητή προϋπόθεση ότι δεν θα κοινοποιηθούν στη CERT-ΕΕ.

Άρθρο 21

Συντονισμός της αντιμετώπισης περιστατικών και συνεργασία σε σημαντικά περιστατικά

1. Ενεργώντας ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας, η CERT-ΕΕ διευκολύνει την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά μεταξύ:

   α) των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης·

   β) των ομολόγων της που αναφέρονται στα άρθρα 16 και 17.

2. Η CERT-ΕΕ διευκολύνει τον συντονισμό μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης για την αντιμετώπιση περιστατικών, μεταξύ άλλων, με:

   α) συμβολή σε συνεπή εξωτερική επικοινωνία·

   β) αμοιβαία συνδρομή·

   γ) βέλτιστη χρήση επιχειρησιακών πόρων·

   δ) συντονισμό με άλλους μηχανισμούς αντιμετώπισης κρίσεων σε επίπεδο Ένωσης.

3. Η CERT-ΕΕ στηρίζει τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης όσον αφορά την επίγνωση της κατάστασης σχετικά με τις κυβερνοαπειλές, τα τρωτά σημεία και τα περιστατικά.

4. Το ΙΙCB εκδίδει έγγραφα καθοδήγησης σχετικά με τον συντονισμό της αντιμετώπισης περιστατικών και τη συνεργασία για σημαντικά περιστατικά. Όταν υπάρχουν υπόνοιες ότι ένα περιστατικό έχει ποινικό χαρακτήρα, η CERT-ΕΕ παρέχει συμβουλές σχετικά με τον τρόπο αναφοράς του περιστατικού στις αρχές επιβολής του νόμου.

Άρθρο 22

Σοβαρές επιθέσεις

1. Η CERT-ΕΕ συντονίζει τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης κατά την αντιμετώπιση σοβαρών επιθέσεων. Τηρεί κατάλογο της τεχνικής εμπειρογνωσίας που απαιτείται για την αντιμετώπιση περιστατικών σε περίπτωση τέτοιων επιθέσεων.

2. Τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης συμβάλλουν στην κατάρτιση του καταλόγου τεχνικής εμπειρογνωσίας παρέχοντας και επικαιροποιώντας σε ετήσια βάση κατάλογο των διαθέσιμων εμπειρογνωμόνων στο πλαίσιο των αντίστοιχων οργανισμών τους, στον οποίον αναφέρονται λεπτομερώς οι ειδικές τεχνικές δεξιότητές τους.

3. Αφού διασφαλίσει την έγκριση των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, η CERT-ΕΕ δύναται επίσης να ζητήσει από τους εμπειρογνώμονες του καταλόγου που αναφέρεται στην παράγραφο 2 να συμβάλλουν

στην αντιμετώπιση σοβαρής επίθεσης σε κράτος μέλος, σύμφωνα με τις επιχειρησιακές διαδικασίες της Κοινής Κυβερνομονάδας.

Κεφάλαιο VI
ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 23
Αρχική ανακατανομή των πιστώσεων του προϋπολογισμού

Η Επιτροπή προτείνει την ανακατανομή προσωπικού και οικονομικών πόρων από τα σχετικά θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης στον προϋπολογισμό της Επιτροπής. Η ανακατανομή τίθεται σε εφαρμογή ταυτόχρονα με τον πρώτο προϋπολογισμό που θα εγκριθεί μετά την έναρξη ισχύος του παρόντος κανονισμού.

Άρθρο 24
Επανεξέταση

1. Το IICB, με τη συνδρομή της CERT-EE, υποβάλλει περιοδικές εκθέσεις στην Επιτροπή σχετικά με την εφαρμογή του παρόντος κανονισμού. Το IICB μπορεί επίσης να απευθύνει συστάσεις στην Επιτροπή για να προτείνει τροποποιήσεις του παρόντος κανονισμού.

2. Η Επιτροπή υποβάλλει έκθεση σχετικά με την εφαρμογή του παρόντος κανονισμού στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο το αργότερο 48 μήνες μετά την έναρξη ισχύος του παρόντος κανονισμού και στη συνέχεια ανά τριετία.

3. Η Επιτροπή αξιολογεί τη λειτουργία του παρόντος κανονισμού και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών το νωρίτερο πέντε έτη μετά την ημερομηνία έναρξης ισχύος του.

Άρθρο 25
Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες,

Για το Ευρωπαϊκό Κοινοβούλιο	*Για το Συμβούλιο*
Η Πρόεδρος	*Ο Πρόεδρος*

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

1.2. Σχετικοί τομείς πολιτικής

1.3. Η πρόταση/πρωτοβουλία αφορά:

1.4. Στόχοι

1.4.1. Γενικοί στόχοι

1.4.2. Ειδικοί στόχοι

1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις

1.4.4. Δείκτες επιδόσεων

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας

1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.

1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος

1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα

1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

1.7. Προβλεπόμενοι τρόποι διαχείρισης

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

2.2. Συστήματα διαχείρισης και ελέγχου

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις

3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις

3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

ΝΟΜΟΘΕΤΙΚΟ ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

1.1. Τίτλος της πρότασης/πρωτοβουλίας

Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης

1.2. Σχετικοί τομείς πολιτικής

Ευρωπαϊκή δημόσια διοίκηση Η πρόταση αφορά μέτρα που διασφαλίζουν υψηλό κοινό επίπεδο κυβερνοασφάλειας εντός των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης

1.3. Η πρόταση/πρωτοβουλία αφορά:

☑νέα δράση

☐ νέα δράση μετά από πιλοτικό έργο / προπαρασκευαστική ενέργεια[10]

☐ την παράταση υφιστάμενης δράσης

☑ συγχώνευση ή αναπροσανατολισμό μίας ή περισσότερων δράσεων προς άλλη/νέα δράση

1.4. Στόχοι

1.4.1. Γενικοί στόχοι

– Θέσπιση πλαισίου για τη διασφάλιση υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης – Παροχή νέας νομικής βάσης για τη CERT-ΕΕ ώστε να ενισχυθούν η σταθερότητα και η χρηματοδότησή της

1.4.2. Ειδικοί στόχοι

1) Ορισμός υποχρεώσεων βάσει των οποίων τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης οφείλουν να θεσπίσουν εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας

2) Ορισμός υποχρεώσεων βάσει των οποίων τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης υποβάλλουν εκθέσεις σχετικά με το οικείο πλαίσιο

[10] Όπως αναφέρεται στο άρθρο 58 παράγραφος 2 στοιχείο α) ή β) του δημοσιονομικού κανονισμού.

διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, καθώς και με τα περιστατικά κυβερνοασφάλειας

3) Ορισμός κανόνων σχετικά με την οργάνωση και τη λειτουργία του Κέντρου Κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-ΕΕ) και σχετικά με την οργάνωση και τη λειτουργία του διοργανικού συμβουλίου κυβερνοασφάλειας (IICB)

4) Συμβολή στην Κοινή Κυβερνομονάδα

1.4.3. Αναμενόμενα αποτελέσματα και επιπτώσεις

Να προσδιοριστούν τα αποτελέσματα που αναμένεται να έχει η πρόταση/πρωτοβουλία όσον αφορά τους/τις στοχευόμενους/-ες δικαιούχους/ομάδες.

– Εσωτερικά πλαίσια διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, βασικές δέσμες κανόνων κυβερνοασφάλειας, τακτικές αξιολογήσεις του επιπέδου ωριμότητας και σχέδια κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης – Βελτίωση των ικανοτήτων ανθεκτικότητας και αντιμετώπισης περιστατικών στον τομέα της κυβερνοασφάλειας των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης – Εκσυγχρονισμός της CERT-ΕΕ – Συμβολή στην Κοινή Κυβερνομονάδα

1.4.4. Δείκτες επιδόσεων

Να προσδιοριστούν οι δείκτες για την παρακολούθηση της προόδου και των επιτευγμάτων.

– Πλαίσια και βασικές δέσμες κανόνων που θεσπίζονται, τακτικές αξιολογήσεις του επιπέδου ωριμότητας και σχέδια κυβερνοασφάλειας που εκπονούνται στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης – Βελτίωση του χειρισμού περιστατικών – Αυξημένη επίγνωση των κινδύνων κυβερνοασφάλειας στο ανώτερο διοικητικό επίπεδο των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης – Εξισορρόπηση των δαπανών για την ασφάλεια ΤΠΕ ως ποσοστού των συνολικών δαπανών ΤΠΕ – Ισχυρή ηγεσία του IICB και της CERT-ΕΕ – Αυξημένη ανταλλαγή πληροφοριών μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης και με τους σχετικούς φορείς και τα ενδιαφερόμενα μέρη στην ΕΕ – Αυξημένη συνεργασία στον τομέα της κυβερνοασφάλειας με τους σχετικούς φορείς και τα ενδιαφερόμενα μέρη στην ΕΕ, μέσω της CERT-ΕΕ και του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)

1.5. Αιτιολόγηση της πρότασης/πρωτοβουλίας

1.5.1. Βραχυπρόθεσμη ή μακροπρόθεσμη κάλυψη αναγκών, συμπεριλαμβανομένου λεπτομερούς χρονοδιαγράμματος για τη σταδιακή υλοποίηση της πρωτοβουλίας.

Σκοπός της πρότασης είναι η αύξηση του επιπέδου κυβερνοανθεκτικότητας των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, η μείωση των ασυνεπειών όσον αφορά την ανθεκτικότητα σε όλες τις εν λόγω οντότητες και η βελτίωση του επιπέδου κοινής επίγνωσης της κατάστασης και της συλλογικής ικανότητας προετοιμασίας και αντιμετώπισης.

Η πρόταση συμφωνεί και συνάδει πλήρως με άλλες σχετικές πρωτοβουλίες, ιδίως με την πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (πρόταση οδηγίας NIS 2).

Η πρόταση αποτελεί ουσιώδες μέρος της στρατηγικής της ΕΕ για την Ένωση Ασφάλειας και της στρατηγικής κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία.

Ο κανονισμός προβλέπεται να προταθεί από την Ευρωπαϊκή Επιτροπή τον Οκτώβριο του 2021, η έκδοση του κανονισμού από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο αναμένεται το 2022, και οι διατάξεις θα αρχίσουν να εφαρμόζονται με την έναρξη ισχύος του κανονισμού. Οι δημοσιονομικές επιπτώσεις και οι επιπτώσεις στους ανθρώπινους πόρους που περιγράφονται στο παρόν νομοθετικό δημοσιονομικό δελτίο προβλέπεται να αρχίσουν το 2023. Ξεκίνησε ήδη μια περίοδος προπαρασκευής το 2021, αλλά οι δραστηριότητες προπαρασκευής των ετών 2021 και 2022 δεν εμπίπτουν στις δημοσιονομικές επιπτώσεις της πρότασης.

1.5.2. Προστιθέμενη αξία της ενωσιακής παρέμβασης (που μπορεί να προκύπτει από διάφορους παράγοντες, π.χ. οφέλη από τον συντονισμό, ασφάλεια δικαίου, μεγαλύτερη αποτελεσματικότητα ή συμπληρωματικότητα). Για τους σκοπούς του παρόντος σημείου «προστιθέμενη αξία της ενωσιακής παρέμβασης» είναι η αξία που απορρέει από την ενωσιακή παρέμβαση και η οποία προστίθεται στην αξία που θα είχε δημιουργηθεί αν τα κράτη μέλη ενεργούσαν μεμονωμένα.

Λόγοι για ανάληψη δράσης σε ευρωπαϊκό επίπεδο (εκ των προτέρων)

Από το 2019 έως το 2021, ο αριθμός των σημαντικών περιστατικών που επηρέασαν τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης και πραγματοποιήθηκαν από παράγοντες προηγμένων επίμονων απειλών αυξήθηκε κατακόρυφα. Ο αριθμός των σημαντικών περιστατικών που σημειώθηκαν κατά το πρώτο εξάμηνο του 2021 ήταν αντίστοιχος του αριθμού που καταγράφηκε ολόκληρο το 2020. Αυτό αντικατοπτρίζεται επίσης στον αριθμό των εικόνων εγκληματολογικής έρευνας (στιγμιότυπα του περιεχομένου των επηρεαζόμενων συστημάτων ή συσκευών) τις οποίες ανέλυσε η CERT-ΕΕ το 2020, ο οποίος τριπλασιάστηκε σε σύγκριση με το 2019, ενώ ο αριθμός των σημαντικών περιστατικών υπερδεκαπλασιάστηκε από το 2018.

Τα επίπεδα ωριμότητας στον τομέα της κυβερνοασφάλειας διαφέρουν σημαντικά από τη μία οντότητα στην άλλη[11]. Ο παρών κανονισμός διασφαλίζει ότι όλα τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης θα εφαρμόζουν μια βασική δέσμη κανόνων ασφάλειας και θα συνεργάζονται μεταξύ τους με στόχο την ανοικτή και αποτελεσματική λειτουργία της ενωσιακής διοίκησης.

Τα συστήματα που πρέπει να διαφυλαχθούν εμπίπτουν στην αυτονομία των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης και τελούν υπό τη διαχείρισή αυτών· οι προτεινόμενες δράσεις δεν μπορούν να αναληφθούν από τα κράτη μέλη.

1.5.3. Διδάγματα από ανάλογες εμπειρίες του παρελθόντος

Η οδηγία NIS είναι το πρώτο οριζόντιο μέσο για την εσωτερική αγορά που αποσκοπεί στη βελτίωση της ανθεκτικότητας των δικτύων και των συστημάτων στην Ένωση έναντι των κινδύνων κυβερνοασφάλειας. Από την έναρξη ισχύος της το 2016, έχει συμβάλει σημαντικά στην αύξηση του κοινού επιπέδου κυβερνοασφάλειας μεταξύ των κρατών μελών. Η πρόταση οδηγίας NIS 2 αποσκοπεί στην περαιτέρω βελτίωση των μέτρων αυτών.

Επιδίωξη του κανονισμού είναι να προβλεφθούν παρόμοια μέτρα για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

1.5.4. Συμβατότητα με το πολυετές δημοσιονομικό πλαίσιο και ενδεχόμενες συνέργειες με άλλα κατάλληλα μέσα

Η πρόταση συνάδει με το πολυετές δημοσιονομικό πλαίσιο και αποτελεί ουσιώδες μέρος της στρατηγικής της ΕΕ για την Ένωση Ασφάλειας και της στρατηγικής κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία.

Η πρόταση προβλέπει την εφαρμογή μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης. Η πρόταση συνάδει με την πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (πρόταση οδηγίας NIS 2).

1.5.5. Αξιολόγηση των διαφόρων διαθέσιμων επιλογών χρηματοδότησης, συμπεριλαμβανομένων των δυνατοτήτων ανακατανομής

Για τη διαχείριση των καθηκόντων από τη CERT-ΕΕ απαιτούνται ειδικά προφίλ και συμπληρωματικός φόρτος εργασίας που δεν μπορεί να καλυφθεί χωρίς αύξηση των ανθρώπινων και οικονομικών πόρων.

[11] Βλέπε: [Ειδική έκθεση του ΕΕΣ για την κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης].

1.6. Διάρκεια και δημοσιονομικές επιπτώσεις της πρότασης/πρωτοβουλίας

☐ **περιορισμένη διάρκεια**

– ☐ με ισχύ από [HH/MM]EEEE έως [HH/MM]EEEE

– ☐ Δημοσιονομικές επιπτώσεις από το EEEE έως το EEEE για πιστώσεις αναλήψεων υποχρεώσεων και από το EEEE έως το EEEE για πιστώσεις πληρωμών.

☑ **απεριόριστη διάρκεια**

– Οι δημοσιονομικές επιπτώσεις αναμένεται να αρχίσουν με τον πρώτο προϋπολογισμό που θα εγκριθεί έπειτα από την έναρξη ισχύος του κανονισμού. Η ανακατανομή των πόρων από τα θεσμικά και λοιπά κύρια όργανα της Ένωσης στην Επιτροπή θα πραγματοποιηθεί κατά το πρώτο έτος, το οποίο θεωρείται μεταβατικό έτος· η ανωτέρω και άλλες (ανα)κατανομές πόρων θα πραγματοποιούνται στο πλαίσιο των ετήσιων προϋπολογισμών. Εάν ο κανονισμός εκδοθεί το 2022, το οικονομικό έτος 2023 θα αποτελέσει τη μεταβατική περίοδο και το 2024 θα ξεκινήσει η λειτουργία σε πλήρη κλίμακα.

1.7. Προβλεπόμενοι τρόποι διαχείρισης[12]

☑ **Άμεση διαχείριση** από την Επιτροπή και από κάθε θεσμικό και λοιπό όργανο και οργανισμό της Ένωσης

– ☑ από τις υπηρεσίες της, συμπεριλαμβανομένου του προσωπικού της στις αντιπροσωπείες της Ένωσης

– ☐ από τους εκτελεστικούς οργανισμούς

☐ **Επιμερισμένη διαχείριση** με τα κράτη μέλη

☐ **Έμμεση διαχείριση** με ανάθεση καθηκόντων εκτέλεσης του προϋπολογισμού:

– ☐ σε τρίτες χώρες ή οργανισμούς που αυτές έχουν ορίσει

– ☐ σε διεθνείς οργανισμούς και στις οργανώσεις τους (να προσδιοριστούν)

– ☐ στην ΕΤΕπ και στο Ευρωπαϊκό Ταμείο Επενδύσεων

– ☐ στους οργανισμούς που αναφέρονται στα άρθρα 70 και 71 του δημοσιονομικού κανονισμού

– ☐ σε οργανισμούς δημοσίου δικαίου

– ☐ σε οργανισμούς που διέπονται από ιδιωτικό δίκαιο και έχουν αποστολή δημόσιας υπηρεσίας, στον βαθμό που παρέχουν επαρκείς οικονομικές εγγυήσεις

[12] Οι λεπτομέρειες σχετικά με τους τρόπους διαχείρισης και οι παραπομπές στον δημοσιονομικό κανονισμό είναι διαθέσιμες στον δικτυακό τόπο BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EL/man/budgmanag/Pages/budgmanag.aspx

– ☐ σε οργανισμούς που διέπονται από το ιδιωτικό δίκαιο κράτους μέλους, στους οποίους έχει ανατεθεί η εκτέλεση σύμπραξης δημόσιου και ιδιωτικού τομέα και οι οποίοι παρέχουν επαρκείς οικονομικές εγγυήσεις

– ☐ σε πρόσωπα επιφορτισμένα με την εφαρμογή συγκεκριμένων δράσεων στην ΚΕΠΠΑ βάσει του τίτλου V της ΣΕΕ και τα οποία προσδιορίζονται στην αντίστοιχη βασική πράξη

– *Αν αναφέρονται περισσότεροι του ενός τρόποι διαχείρισης, να διευκρινιστούν στο τμήμα «Παρατηρήσεις».*

Παρατηρήσεις

Για την εφαρμογή των διοικητικών και δημοσιονομικών διαδικασιών, η CERT-ΕΕ ενεργεί υπό τον έλεγχο της Επιτροπής.

Πρόσθετοι πόροι που προκύπτουν από το σχέδιο κανονισμού:

Η εφαρμογή των άρθρων 12 και 13 του σχεδίου κανονισμού οδηγεί σε διευρυμένο κατάλογο υπηρεσιών με πρόσθετες βασικές υπηρεσίες. Κατά τη λειτουργία σε πλήρη κλίμακα, θα απαιτηθούν οι ακόλουθοι πρόσθετοι πόροι (έως την ολοκλήρωση του ΠΔΠ στο τέλος του 2027): 21 ΙΠΑ και 14,05 εκατ. EUR.

Η κατανομή των πρόσθετων πόρων του προϋπολογισμού στα διάφορα καθήκοντα έχει ως εξής:

α) Για την εκτέλεση των καθηκόντων για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που περιγράφονται στο άρθρο 12 παράγραφος 2 στοιχεία α), β), γ) και ε): 13,75 ΙΠΑ και 11,275 εκατ. EUR.

β) Για την εκτέλεση των καθηκόντων που περιγράφονται στο άρθρο 12 παράγραφος 3 (συμβολή στην Κοινή Κυβερνομονάδα): 2 ΙΠΑ και 381 000 EUR.

γ) Για την εκτέλεση των καθηκόντων που περιγράφονται στο άρθρο 12 παράγραφος 4 (διαρθρωμένη συνεργασία με τον ENISA): 0,25 ΙΠΑ και 236 000 EUR.

δ) Για την εκτέλεση των καθηκόντων που περιγράφονται στο άρθρο 12 παράγραφος 6 (ασκήσεις κυβερνοασφάλειας): 0,25 ΙΠΑ και 79 000 EUR.

ε) Για την εκτέλεση των καθηκόντων που περιγράφονται στο άρθρο 12 παράγραφος 2 στοιχείο δ) και στο άρθρο 13 (ανάλυση και υποβολή εκθέσεων σχετικά με την εφαρμογή του κανονισμού, κατάρτιση εγγράφων καθοδήγησης, συστάσεων και εκκλήσεων για ανάληψη δράσης): 3,75 ΙΠΑ και 2,079 εκατ. EUR.

στ) Για την εκτέλεση καθηκόντων γραμματειακής υποστήριξης του διοργανικού συμβουλίου κυβερνοασφάλειας (IICB): 1 ΙΠΑ.

Επισκόπηση των τρεχόντων πόρων και μετάβαση σε πλήρη κλίμακα:

Τον Σεπτέμβριο του 2021 η CERT-ΕΕ λειτουργούσε με τους κάτωθι πόρους:

— μόνιμο και αποσπασμένο προσωπικό: 14 ΙΠΑ,

— συμβασιούχοι υπάλληλοι που χρηματοδοτούνται βάσει συμφωνιών επιπέδου υπηρεσιών: 24 ΙΠΑ,

— σύνολο 38 ΙΠΑ.

Ο προϋπολογισμός της CERT-ΕΕ για το 2020 είχε ως εξής: 250 000 EUR στο πλαίσιο του προϋπολογισμού της Επιτροπής, 3,5 εκατ. EUR μέσω εσόδων για ειδικό προορισμό από συμφωνίες επιπέδου υπηρεσιών. Σύνολο: 3,75 εκατ. EUR. Πρόκειται για το σύνολο του προϋπολογισμού της CERT-ΕΕ που κάλυπτε την κατάρτιση, το υλισμικό, το λογισμικό, τις αποστολές, τη στήριξη, τους συμβασιούχους υπαλλήλους και τις διασκέψεις.

Όταν τεθεί σε ισχύ ο κανονισμός, οι μελλοντικοί πόροι της CERT-ΕΕ προβλέπεται ότι θα έχουν ως εξής:

— μόνιμο προσωπικό: 34 ΙΠΑ,

— συμβασιούχοι υπάλληλοι: 15 ΙΠΑ,

— σύνολο 49 ΙΠΑ, δηλαδή καθαρή αύξηση 11 ΙΠΑ.

Η μεταβολή της αναλογίας μεταξύ μόνιμου προσωπικού και συμβασιούχων υπαλλήλων οφείλεται στην αντιμετώπιση της σχετικής δυσκολίας όσον αφορά την πρόσληψη και τη διατήρηση επαγγελματιών υψηλού επιπέδου στον τομέα της κυβερνοασφάλειας λόγω του ότι σπανίζουν στην αγορά εργασίας.

Επιπλέον, θα απαιτηθεί 1 ΙΠΑ συμβασιούχου υπαλλήλου εντός της Γενικής Διεύθυνσης Πληροφορικής της Επιτροπής για την υποστήριξη του ΙΙCB (του διοργανικού συμβουλίου κυβερνοασφάλειας).

Ως εκ τούτου, θα απαιτηθούν συνολικά 21 ΙΠΑ για την εφαρμογή του κανονισμού (20 ΙΠΑ για τη CERT-ΕΕ και 1 ΙΠΑ για τη Γενική Διεύθυνση Πληροφορικής της Επιτροπής). Αυτό θα αντισταθμιστεί με παράλληλη μείωση 9 ΙΠΑ συμβασιούχων υπαλλήλων στη CERT-ΕΕ, οι οποίοι προηγουμένως χρηματοδοτούνταν μέσω εσόδων για ειδικό προορισμό από συμφωνίες επιπέδου υπηρεσιών.

Ο προϋπολογισμός της CERT-ΕΕ για τους μη ανθρώπινους πόρους το 2024 μετά τη μεταβατική περίοδο θα καλύψει τα καθήκοντα που απαριθμούνται ανωτέρω στα στοιχεία α) έως ε) και προβλέπεται να χρηματοδοτηθεί ως εξής:

— 8,921 εκατ. EUR ετησίως από τα θεσμικά όργανα της Ένωσης που χρηματοδοτούνται από τον τομέα 7 του προϋπολογισμού της Ένωσης,

— 2,459 εκατ. EUR από τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης που χρηματοδοτούνται από τους τομείς 1 έως 6 του προϋπολογισμού της Ένωσης,

— 2,670 εκατ. EUR από αυτοχρηματοδοτούμενα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

— Σύνολο προϋπολογισμού της CERT-ΕΕ: 14,05 εκατ. EUR.

Τα καθήκοντα που απαριθμούνται στο άρθρο 12 παράγραφος 5 δεν περιγράφονται στον κατάλογο υπηρεσιών της, καθώς πρόκειται για χρεώσιμες υπηρεσίες. Οι υπηρεσίες αυτές

είναι επικουρικές, αντιπροσωπεύουν σχετικά χαμηλά ποσά, είναι ως επί το πλείστον προσωρινές και το κόστος τους θα ανακτηθεί από τους δικαιούχους των υπηρεσιών μέσω συμφωνιών επιπέδου υπηρεσιών ή γραπτών συμφωνιών.

Όσον αφορά τις συνεισφορές στο προσωπικό της CERT-ΕΕ: τα θεσμικά και λοιπά κύρια όργανα της Ένωσης συνεισφέρουν δίκαια ανάλογα με το αντίστοιχο ποσοστό των μόνιμων θέσεων AD του οργανισμού. Θα πρέπει να εξεταστεί αν η ΕΚΤ και η ΕΤΕπ μπορούν επίσης να συνεισφέρουν δίκαια μέσω της απόσπασης μόνιμου προσωπικού.

2. ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ

2.1. Κανόνες παρακολούθησης και υποβολής εκθέσεων

Να προσδιοριστούν η συχνότητα και οι όροι.

Η Επιτροπή, με τη βοήθεια του IICB και της CERT-EE, θα επανεξετάζει περιοδικά τη λειτουργία του κανονισμού και θα υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο για πρώτη φορά το αργότερο 48 μήνες από την έναρξη ισχύος του παρόντος κανονισμού και στη συνέχεια ανά τριετία.

Οι πηγές δεδομένων που χρησιμοποιούνται για τις επανεξετάσεις θα είναι κυρίως από το IICB και τη CERT-EE. Επιπλέον, θα μπορούσαν να χρησιμοποιηθούν ειδικά εργαλεία συλλογής δεδομένων όποτε χρειάζεται, π.χ. έρευνες των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, του ENISA ή του δικτύου CSIRT.

2.2. Συστήματα διαχείρισης και ελέγχου

2.2.1. Αιτιολόγηση των τρόπων διαχείρισης, των μηχανισμών εκτέλεσης της χρηματοδότησης, των όρων πληρωμής και της προτεινόμενης στρατηγικής ελέγχου

Η διαχείριση των δράσεων που απορρέουν από τον κανονισμό θα πραγματοποιείται στο πλαίσιο κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης σύμφωνα με τους οικείους εφαρμοστέους κανόνες και κανονισμούς.

Η διοικητική και δημοσιονομική διαχείριση των δραστηριοτήτων της CERT-EE είναι ενσωματωμένη στη διοίκηση της Επιτροπής και ακολουθεί τους εφαρμοστέους μηχανισμούς διαχείρισης και εφαρμογής, τους τρόπους πληρωμής και τους ελέγχους της Επιτροπής.

Ο εσωτερικός ελεγκτής της Επιτροπής ασκεί τις ίδιες εξουσίες έναντι της CERT-EE όπως και έναντι των υπηρεσιών της Επιτροπής.

2.2.2. Πληροφορίες σχετικά με τους κινδύνους που έχουν εντοπιστεί και τα συστήματα εσωτερικού ελέγχου που έχουν δημιουργηθεί για τον μετριασμό τους

Πολύ χαμηλός κίνδυνος, δεδομένου ότι η CERT-EE είναι ήδη διοικητικά συνδεδεμένη ως ειδική ομάδα της Επιτροπής με τον γενικό διευθυντή πληροφορικής, και το IICB ακολουθεί το πρότυπο της υφιστάμενης διοικούσας επιτροπής της CERT-EE. Ως εκ τούτου, το οικοσύστημα για τη δημοσιονομική διαχείριση και τον εσωτερικό έλεγχο έχει ήδη δημιουργηθεί.

2.2.3. Εκτίμηση και αιτιολόγηση της οικονομικής αποδοτικότητας των ελέγχων (λόγος του κόστους του ελέγχου προς την αξία των σχετικών κονδυλίων που αποτελούν αντικείμενο διαχείρισης) και αξιολόγηση του εκτιμώμενου επιπέδου κινδύνου σφάλματος (κατά την πληρωμή και κατά το κλείσιμο)

Οι διαδικασίες για τη σύναψη συμβάσεων, τη δημοσιονομική διαχείριση και τον έλεγχο έχουν ήδη τεθεί σε εφαρμογή και έχουν δοκιμαστεί επαρκώς. Η οικονομική αποδοτικότητα των ελέγχων και τα επίπεδα κινδύνου σφάλματος αντιστοιχούν σε

εκείνα κάθε θεσμικού και λοιπού οργάνου και οργανισμού της Ένωσης, καθώς και σε εκείνα της Επιτροπής για τις δραστηριότητες της CERT-EE.

2.3. Μέτρα για την πρόληψη περιπτώσεων απάτης και παρατυπίας

Να προσδιοριστούν τα ισχύοντα ή τα προβλεπόμενα μέτρα πρόληψης και προστασίας, π.χ. στη στρατηγική για την καταπολέμηση της απάτης.

Τα συστήματα δημοσιονομικής διαχείρισης και εσωτερικού ελέγχου της Επιτροπής εφαρμόζονται στις δραστηριότητες της CERT-EE.

Για την καταπολέμηση της απάτης, της διαφθοράς και άλλων παράνομων δραστηριοτήτων, εφαρμόζονται άνευ περιορισμών οι διατάξεις του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Σεπτεμβρίου 2013, σχετικά με τις έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF).

3. ΕΚΤΙΜΩΜΕΝΕΣ ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΠΡΟΤΑΣΗΣ/ΠΡΩΤΟΒΟΥΛΙΑΣ

3.1. Τομείς του πολυετούς δημοσιονομικού πλαισίου και γραμμές δαπανών του προϋπολογισμού που επηρεάζονται

- Υφιστάμενες γραμμές του προϋπολογισμού

<u>Κατά σειρά</u> τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ[13].	χωρών ΕΖΕΣ[14]	υποψηφίων για ένταξη χωρών[15]	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού
1 έως 6	Γραμμές του προϋπολογισμού που καλύπτουν τις συνεισφορές της Ένωσης σε αποκεντρωμένους οργανισμούς και όργανα	ΔΠ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
7	Γραμμές του προϋπολογισμού που καλύπτουν τις αποδοχές του προσωπικού, τις δαπάνες ΤΠ και άλλες διοικητικές δαπάνες στα διάφορα τμήματα του προϋπολογισμού της ΕΕ	ΜΔΠ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

- Νέες γραμμές του προϋπολογισμού, των οποίων έχει ζητηθεί η δημιουργία

<u>Κατά σειρά</u> τομέων του πολυετούς δημοσιονομικού πλαισίου και γραμμών του προϋπολογισμού

Τομέας του πολυετούς δημοσιονομικού πλαισίου	Γραμμή του προϋπολογισμού	Είδος δαπάνης	Συμμετοχή			
	Αριθμός	ΔΠ/ΜΔΠ	χωρών ΕΖΕΣ	υποψηφίων για ένταξη χωρών	τρίτων χωρών	κατά την έννοια του άρθρου 21 παράγραφος 2 στοιχείο β) του δημοσιονομικού κανονισμού
	Καμία		ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ	ΝΑΙ/ΟΧΙ

[13] ΔΠ = Διαχωριζόμενες πιστώσεις / ΜΔΠ = Μη διαχωριζόμενες πιστώσεις.
[14] ΕΖΕΣ: Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών.
[15] Υποψήφιες χώρες και, κατά περίπτωση, δυνάμει υποψήφια μέλη των Δυτικών Βαλκανίων.

3.2. Εκτιμώμενες δημοσιονομικές επιπτώσεις της πρότασης στις πιστώσεις

3.2.1. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις επιχειρησιακές πιστώσεις

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση επιχειρησιακών πιστώσεων, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Τομέας του πολυετούς δημοσιονομικού πλαισίου	1 έως 6	Τομείς που καλύπτουν τις συνεισφορές σε αποκεντρωμένους οργανισμούς και όργανα

ΓΔ: Αρκετές			Έτος **2023**	Έτος **2024**	Έτος **2025**	Έτος **2026**	Έτος **2027**	**ΣΥΝΟΛΟ**
○ Επιχειρησιακές πιστώσεις								
Γραμμές του προϋπολογισμού που καλύπτουν τις συνεισφορές της Ένωσης σε αποκεντρωμένους οργανισμούς και φορείς (xx 10 xx xx)[16]	Αναλήψεις υποχρεώσεων	(1α)	2,459	2,459	2,459	2,459	2,459	12,293
	Πληρωμές	(2α)	2,459	2,459	2,459	2,459	2,459	12,293
Πιστώσεις διοικητικού χαρακτήρα χρηματοδοτούμενες από το κονδύλιο ειδικών προγραμμάτων[17]								
Γραμμή του προϋπολογισμού		(3)						
ΣΥΝΟΛΟ πιστώσεων	Αναλήψεις υποχρεώσεων	=1α+1 β+3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Σύμφωνα με την επίσημη ονοματολογία του προϋπολογισμού.

[17] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

για τη ΓΔ: Αρκετές	Πληρωμές	=2α+2β+3	2,459	2,459	2,459	2,459	2,459	12,293

○ ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων	Αναλήψεις υποχρεώσεων	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Πληρωμές	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων		(6)						
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 6 του πολυετούς δημοσιονομικού πλαισίου	Αναλήψεις υποχρεώσεων	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Πληρωμές	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Αν η πρόταση/πρωτοβουλία επηρεάζει περισσότερους του ενός επιχειρησιακούς τομείς, επαναλάβετε το ανωτέρω τμήμα:

○ ΣΥΝΟΛΟ επιχειρησιακών πιστώσεων (όλοι οι επιχειρησιακοί τομείς)	Αναλήψεις υποχρεώσεων	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Πληρωμές	(5)	2,459	2,459	2,459	2,459	2,459	12,293
ΣΥΝΟΛΟ πιστώσεων διοικητικού χαρακτήρα χρηματοδοτούμενων από το κονδύλιο ειδικών προγραμμάτων (όλοι οι επιχειρησιακοί τομείς)		(6)						
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 6 του πολυετούς δημοσιονομικού πλαισίου (ποσό αναφοράς)	Αναλήψεις υποχρεώσεων	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Πληρωμές	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Τομέας του πολυετούς δημοσιονομικού πλαισίου	**7**	«Διοικητικές δαπάνες»

Αυτό το τμήμα πρέπει να συμπληρωθεί με «στοιχεία διοικητικού χαρακτήρα του προϋπολογισμού» τα οποία θα εισαχθούν, καταρχάς, στο παράρτημα του νομοθετικού δημοσιονομικού δελτίου (παράρτημα V του εσωτερικού κανονισμού), που τηλεφορτώνεται στο DECIDE για διυπηρεσιακή διαβούλευση.

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		Έτος **2023**	Έτος **2024**	Έτος **2025**	Έτος **2026**	**Έτος 2027**	**ΣΥΝΟΛΟ**
ΓΔ: DIGIT (CERT-EE)							
○ Ανθρώπινοι πόροι		1,184	2,126	2,754	3,225	3,225	12,514
○ Άλλες διοικητικές δαπάνες		7,938	8,921	8,921	8,921	8,921	43,622
ΣΥΝΟΛΟ ΓΔ DIGIT (CERT-EE)	Πιστώσεις	9,122	11,047	11,675	12,146	12,146	56,136

ΣΥΝΟΛΟ πιστώσεων του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	(Σύνολο αναλήψεων υποχρεώσεων = Σύνολο πληρωμών)	9,122	11,047	11,675	12,146	12,146	**56,136**

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

		Έτος 2023	Έτος 2024	Έτος 2025	Έτος 2026	Έτος 2027	**ΣΥΝΟΛΟ**
ΣΥΝΟΛΟ πιστώσεων των ΤΟΜΕΩΝ 1 έως 7 του πολυετούς δημοσιονομικού πλαισίου (*)	Αναλήψεις υποχρεώσεων	11,581	13,506	14,134	14,605	14,605	68,429
	Πληρωμές	11,581	13,506	14,134	14,605	14,605	68,429

(*) Οι συνεισφορές των αυτοχρηματοδοτούμενων θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης εκτιμώνται σε 2,670 εκατ. EUR ετησίως (σύνολο για τα πέντε έτη, 13,350 εκατ. EUR). Οι συνεισφορές θα αποτελούν έσοδα για ειδικό προορισμό για τη CERT-EE. Οι ανωτέρω πίνακες περιλαμβάνουν μόνο τις εκτιμώμενες συνολικές επιπτώσεις στον προϋπολογισμό της Ένωσης και δεν περιλαμβάνουν τις εν λόγω συνεισφορές.

3.2.2. Εκτιμώμενο αποτέλεσμα που χρηματοδοτείται με επιχειρησιακές πιστώσεις

Πιστώσεις αναλήψεων υποχρεώσεων σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Να προσδιοριστούν οι στόχοι και τα αποτελέσματα			Έτος **N**		Έτος **N+1**		Έτος **N+2**		Έτος **N+3**		Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)						**ΣΥΝΟΛΟ**	
	ΑΠΟΤΕΛΕΣΜΑΤΑ																	
⇩	Είδος [18]	Μέσο κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Αριθ.	Κόστος	Συνολικός αριθ.	Συνολικό κόστος
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 1[19]…																		
- Αποτέλεσμα																		
- Αποτέλεσμα																		
- Αποτέλεσμα																		
Μερικό σύνολο για τον ειδικό στόχο αριθ. 1																		
ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ αριθ. 2 ...																		
- Αποτέλεσμα																		
Μερικό σύνολο για τον ειδικό																		

[18] Τα αποτελέσματα είναι τα προϊόντα και οι υπηρεσίες που θα παρασχεθούν (π.χ.: αριθμός ανταλλαγών φοιτητών που θα χρηματοδοτηθούν, αριθμός χλμ. οδών που θα κατασκευαστούν κ.λπ.).

[19] Όπως περιγράφεται στο σημείο 1.4.2. «Ειδικοί στόχοι …»

στόχο αριθ. 2																
ΣΥΝΟΛΑ																

3.2.3. Συνοπτική παρουσίαση των εκτιμώμενων επιπτώσεων στις διοικητικές πιστώσεις

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση πιστώσεων διοικητικού χαρακτήρα, όπως εξηγείται κατωτέρω:

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

	Έτος 2023	Έτος 2024	Έτος 2025	Έτος 2026	Έτος 2027	**ΣΥΝΟΛΟ**
ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου						
Ανθρώπινοι πόροι						
Μόνιμοι υπάλληλοι (βαθμοί AD)	1,099	2,041	2,669	3,14	3,14	12,089
Συμβασιούχοι υπάλληλοι	0,085	0,085	0,085	0,085	0,085	0,425
Άλλες διοικητικές δαπάνες	7,938	8,921	8,921	8,921	8,921	43,622
Μερικό σύνολο του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου	9,122	11,047	11,675	12,146	12,146	56,136

Εκτός του ΤΟΜΕΑ 7[20] του πολυετούς δημοσιονομικού πλαισίου						
Ανθρώπινοι πόροι						
Άλλες δαπάνες διοικητικού χαρακτήρα						
Μερικό σύνολο εκτός του ΤΟΜΕΑ 7 του πολυετούς δημοσιονομικού πλαισίου						

ΣΥΝΟΛΟ	9,122	11,047	11,675	12,146	12,146	56,136

Οι απαιτούμενες πιστώσεις για ανθρώπινους πόρους και άλλες δαπάνες διοικητικού χαρακτήρα θα καλυφθούν από τις πιστώσεις της ΓΔ που έχουν ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχουν ανακατανεμηθεί στο εσωτερικό της ΓΔ και οι οποίες θα συμπληρωθούν, κατά περίπτωση, με πρόσθετα κονδύλια που ενδέχεται να χορηγηθούν στην αρμόδια για τη

[20] Τεχνική και/ή διοικητική βοήθεια και δαπάνες στήριξης της εφαρμογής προγραμμάτων και/ή δράσεων της ΕΕ (πρώην γραμμές «ΒΑ»), έμμεση έρευνα, άμεση έρευνα.

διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

3.2.3.1. Εκτιμώμενες ανάγκες σε ανθρώπινους πόρους

– ☐ Η πρόταση/πρωτοβουλία δεν συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων.

– ☑ Η πρόταση/πρωτοβουλία συνεπάγεται τη χρησιμοποίηση ανθρώπινων πόρων, όπως εξηγείται κατωτέρω:

Εκτίμηση η οποία πρέπει να εκφράζεται σε μονάδες ισοδυνάμων πλήρους απασχόλησης

		Έτος 2023	Έτος 2024	Έτος 2025	Έτος 2026	Έτος 2027		
Θέσεις απασχόλησης του πίνακα προσωπικού (θέσεις μόνιμων και έκτακτων υπαλλήλων)								
20 01 02 01 (στην έδρα και στις αντιπροσωπείες της Επιτροπής)		7	13	17	20	20		
20 01 02 03 (στις αντιπροσωπείες της ΕΕ)								
01 01 01 01 (έμμεση έρευνα)								
01 01 01 11 (άμεση έρευνα)								
Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν)								
Εξωτερικό προσωπικό (σε μονάδα ισοδυνάμου πλήρους απασχόλησης: ΙΠΑ)[21]								
20 02 01 (AC, END, INT από το συνολικό κονδύλιο)		1	1	1	1	1		
20 02 03 (AC, AL, END, INT και JPD στις αντιπροσωπείες της ΕΕ)								
XX 01 xx **yy zz** [22]	– στην έδρα:							
	– στις αντιπροσωπείες της ΕΕ							
01 01 01 02 (AC, END, INT – έμμεση έρευνα)								
01 01 01 12 (AC, END, INT – άμεση έρευνα)								
Άλλες γραμμές του προϋπολογισμού (να προσδιοριστούν)								
ΣΥΝΟΛΟ		**8**	**14**	**18**	**21**	**21**		

XX είναι ο σχετικός τομέας πολιτικής ή ο σχετικός τίτλος του προϋπολογισμού.

Οι ανάγκες σε ανθρώπινους πόρους θα καλυφθούν από το προσωπικό της ΓΔ που έχει ήδη διατεθεί για τη διαχείριση της δράσης και/ή έχει ανακατανεμηθεί στο εσωτερικό της ΓΔ, το οποίο θα συμπληρωθεί, αν χρειαστεί, με τυχόν πρόσθετους πόρους που μπορεί να διατεθούν στην αρμόδια για τη διαχείριση ΓΔ στο πλαίσιο της ετήσιας διαδικασίας κατανομής και λαμβανομένων υπόψη των υφιστάμενων δημοσιονομικών περιορισμών.

Περιγραφή των προς εκτέλεση καθηκόντων:

Μόνιμοι και έκτακτοι υπάλληλοι	Οι μόνιμοι υπάλληλοι θα εκτελούν τα καθήκοντα και τις δραστηριότητες της CERT-ΕΕ σύμφωνα με τον κανονισμό, ιδίως τα κεφάλαια IV και V.
Εξωτερικό προσωπικό	Ο συμβασιούχος υπάλληλος θα επικουρεί τα γραμματειακά καθήκοντα του διοργανικού συμβουλίου κυβερνοασφάλειας.

[21] AC = Συμβασιούχος υπάλληλος· AL = Τοπικός υπάλληλος· END = Αποσπασμένος εθνικός εμπειρογνώμονας· INT = Προσωρινό προσωπικό· JPD = Νέος επαγγελματίας σε αντιπροσωπεία της ΕΕ.

[22] Επιμέρους ανώτατο όριο εξωτερικού προσωπικού που καλύπτεται από επιχειρησιακές πιστώσεις (πρώην γραμμές «ΒΑ»).

3.2.4. Συμβατότητα με το ισχύον πολυετές δημοσιονομικό πλαίσιο

Η πρόταση/πρωτοβουλία:

– ☑ μπορεί να χρηματοδοτηθεί εξ ολοκλήρου με ανακατανομή εντός του οικείου τομέα του πολυετούς δημοσιονομικού πλαισίου (ΠΔΠ).

Να εξηγηθεί ο απαιτούμενος αναπρογραμματισμός και να προσδιοριστούν οι σχετικές γραμμές του προϋπολογισμού και τα αντίστοιχα ποσά. Να υποβληθεί πίνακας Excel σε περίπτωση σημαντικού αναπρογραμματισμού.

– ☐ συνεπάγεται τη χρησιμοποίηση του αδιάθετου περιθωρίου στο πλαίσιο του αντίστοιχου τομέα του ΠΔΠ και/ή τη χρήση ειδικών μηχανισμών, όπως ορίζεται στον κανονισμό για το ΠΔΠ.

Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, τα αντίστοιχα ποσά και οι μηχανισμοί που προτείνεται να χρησιμοποιηθούν.

– ☐ συνεπάγεται την αναθεώρηση του ΠΔΠ.

Να εξηγηθούν οι απαιτούμενες ενέργειες και να προσδιοριστούν οι σχετικοί τομείς και οι σχετικές γραμμές του προϋπολογισμού, καθώς και τα αντίστοιχα ποσά.

3.2.5. Συμμετοχή τρίτων στη χρηματοδότηση

Η πρόταση/πρωτοβουλία:

– ☑ δεν προβλέπει συγχρηματοδότηση από τρίτους[23]

– ☐ προβλέπει τη συγχρηματοδότηση από τρίτους που εκτιμάται παρακάτω:

Πιστώσεις σε εκατ. EUR (με τρία δεκαδικά ψηφία)

	Έτος **N**[24]	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)			Σύνολο
Προσδιορισμός του φορέα συγχρηματοδότησης								
ΣΥΝΟΛΟ συγχρηματοδοτούμενων πιστώσεων								

[23] Τα έσοδα για ειδικό προορισμό που προέρχονται από τη σποραδική παροχή υπηρεσιών σε μη συνιστώντες οργανισμούς που προβλέπονται στο άρθρο 12 παράγραφος 5 στοιχείο γ) δεν έχουν εκτιμηθεί διότι αναμένεται να είναι οριακά.

[24] Το έτος Ν είναι το έτος έναρξης εφαρμογής της πρότασης/πρωτοβουλίας. Να αντικατασταθεί το «Ν» με το αναμενόμενο πρώτο έτος εφαρμογής (για παράδειγμα: 2021). Το ίδιο και για τα επόμενα έτη.

3.3. Εκτιμώμενες επιπτώσεις στα έσοδα

– ☑ Η πρόταση/πρωτοβουλία δεν έχει δημοσιονομικές επιπτώσεις στα έσοδα.

– ☐ Η πρόταση/πρωτοβουλία έχει τις δημοσιονομικές επιπτώσεις που περιγράφονται κατωτέρω:

  – ☐ στους ιδίους πόρους

  – ☐ στα λοιπά έσοδα

  – Να αναφερθεί αν τα έσοδα προορίζονται για γραμμές δαπανών ☐

σε εκατ. EUR (με τρία δεκαδικά ψηφία)

Γραμμή εσόδων του προϋπολογισμού:	Διαθέσιμες πιστώσεις για το τρέχον οικονομικό έτος	Επιπτώσεις της πρότασης/πρωτοβουλίας[25]						
		Έτος **N**	Έτος **N+1**	Έτος **N+2**	Έτος **N+3**	Να εγγραφούν όσα έτη απαιτούνται, ώστε να εμφανίζεται η διάρκεια των επιπτώσεων (βλ. σημείο 1.6)		
Άρθρο …….								

Ως προς τα έσοδα «για ειδικό προορισμό», να προσδιοριστούν οι γραμμές δαπανών του προϋπολογισμού που επηρεάζονται.

Άλλες παρατηρήσεις (π.χ. μέθοδος/τύπος για τον υπολογισμό των επιπτώσεων στα έσοδα ή τυχόν άλλες πληροφορίες).

[25] Όσον αφορά τους παραδοσιακούς ιδίους πόρους (δασμούς, εισφορές ζάχαρης), τα αναγραφόμενα ποσά πρέπει να είναι καθαρά ποσά, δηλ. τα ακαθάριστα ποσά μετά την αφαίρεση του 20 % για έξοδα είσπραξης.