ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ **ΤΟ ΣΥΜΒΟΥΛΙΟ**

Στρασβούργο, 13 Δεκεμβρίου 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΓΙΑ ΤΟΝ ΚΑΘΟΡΙΣΜΟ ΜΕΤΡΩΝ ΓΙΑ ΥΨΗΛΟ ΚΟΙΝΟ ΕΠΙΠΕΔΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΑ ΘΕΣΜΙΚΑ ΚΑΙ ΛΟΙΠΑ ΟΡΓΑΝΑ ΚΑΙ ΟΡΓΑΝΙΣΜΟΥΣ ΤΗΣ ΕΝΩΣΗΣ

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ, Ευρατόμ) 2023/…
ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 13ης Δεκεμβρίου 2023

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[1],

[1] Θέση του Ευρωπαϊκού Κοινοβουλίου της 21ης Νοεμβρίου 2023 (δεν έχει δημοσιευτεί ακόμη στην Επίσημη Εφημερίδα) και απόφαση του Συμβουλίου της 8ης Δεκεμβρίου 2023.

Εκτιμώντας τα ακόλουθα:

(1) Στην ψηφιακή εποχή, η τεχνολογία των πληροφοριών και των επικοινωνιών αποτελεί ακρογωνιαίο λίθο μιας ανοικτής, αποτελεσματικής και ανεξάρτητης ευρωπαϊκής διοίκησης. Η εξελισσόμενη τεχνολογία και η αυξημένη πολυπλοκότητα και διασυνδεσιμότητα των ψηφιακών συστημάτων επιτείνουν τους κινδύνους κυβερνοασφάλειας, καθιστώντας τις οντότητες της Ένωσης περισσότερο ευάλωτες σε κυβερνοαπειλές και σχετικά περιστατικά, στοιχείο που απειλεί την επιχειρησιακή τους συνέχεια και την ικανότητά τους να προστατεύουν τα δεδομένα τους. Παρότι η αυξημένη χρήση των υπηρεσιών υπολογιστικού νέφους, η γενικευμένη χρήση της τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ), ο υψηλός βαθμός ψηφιοποίησης, η τηλεργασία και η εξελισσόμενη τεχνολογία και συνδεσιμότητα αποτελούν βασικά χαρακτηριστικά όλων των δραστηριοτήτων των οντοτήτων της Ένωσης, η ψηφιακή ανθεκτικότητα δεν έχει ακόμη αναπτυχθεί επαρκώς.

(2) Το τοπίο των κυβερνοαπειλών που αντιμετωπίζουν οι οντότητες 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 οι παράγοντες απειλής 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 τις ευπάθειες.

(3) Τα περιβάλλοντα ΤΠΕ των οντοτήτων της Ένωσης έχουν αλληλεξαρτήσεις και ενοποιημένες ροές δεδομένων, και οι χρήστες τους συνεργάζονται στενά. Λόγω της διασύνδεσης αυτής, οποιαδήποτε διαταραχή, ακόμη και όταν αρχικά περιορίζεται σε συγκεκριμένη οντότητα της Ένωσης, μπορεί να επιφέρει ευρύτερα αλυσιδωτά αποτελέσματα και να έχει ενδεχομένως ως αποτέλεσμα εκτεταμένες και μακροχρόνιες αρνητικές επιπτώσεις σε άλλες οντότητες της Ένωσης. Επιπλέον, τα περιβάλλοντα ΤΠΕ ορισμένων οντοτήτων της Ένωσης συνδέονται με τα περιβάλλοντα ΤΠΕ των κρατών μελών, με αποτέλεσμα ένα περιστατικό που επηρεάζει μια οντότητα της Ένωσης να ενέχει κίνδυνο για την κυβερνοασφάλεια των περιβαλλόντων ΤΠΕ των κρατών μελών και αντίστροφα. Η ανταλλαγή πληροφοριών σχετικά με συγκεκριμένα περιστατικά μπορεί να διευκολύνει τον εντοπισμό παρόμοιων κυβερνοαπειλών ή περιστατικών που επηρεάζουν τα κράτη μέλη.

(4) Οι οντότητες της Ένωσης αποτελούν ελκυστικούς στόχους και έρχονται αντιμέτωπες 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 των οντοτήτων αυτών. Επομένως, είναι αναγκαίο για τη λειτουργία των οντοτήτων της Ένωσης να επιτύχουν υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω της εφαρμογής μέτρων κυβερνοασφάλειας ανάλογων με τους εντοπισθέντες κινδύνους κυβερνοασφάλειας, της ανταλλαγής πληροφοριών και της συνεργασίας.

(5) Η οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1] αποσκοπεί στην περαιτέρω βελτίωση των ικανοτήτων κυβερνοανθεκτικότητας και αντιμετώπισης περιστατικών των δημόσιων και ιδιωτικών οντοτήτων, των αρμόδιων αρχών και φορέων, καθώς και της Ένωσης στο σύνολό της. Είναι επομένως αναγκαίο να διασφαλιστεί ότι οι οντότητες της Ένωσης ακολουθούν παρόμοια πορεία θεσπίζοντας κανόνες που συμφωνούν με την οδηγία (ΕΕ) 2022/2555 και αντικατοπτρίζουν το επίπεδο φιλοδοξίας της.

(6) Για να επιτευχθεί υψηλό κοινό επίπεδο κυβερνοασφάλειας, είναι αναγκαίο κάθε οντότητα της Ένωσης να θεσπίσει εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας («πλαίσιο»), το οποίο να διασφαλίζει την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας και να λαμβάνει υπόψη την επιχειρησιακή συνέχεια και τη διαχείριση κρίσεων. Το πλαίσιο θα πρέπει να καθορίζει πολιτικές κυβερνοασφάλειας, συμπεριλαμβανομένων στόχων και προτεραιοτήτων, για την ασφάλεια των δικτυακών και πληροφοριακών συστημάτων, που να καλύπτουν το σύνολο του μη διαβαθμισμένου περιβάλλοντος ΤΠΕ. Το πλαίσιο θα πρέπει να βασίζεται σε μια προσέγγιση για όλους τους κινδύνους, η οποία αποσκοπεί στην προστασία των δικτυακών και πληροφοριακών συστημάτων και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από συμβάντα όπως κλοπές, πυρκαγιές, πλημμύρες, διακοπές στις τηλεπικοινωνίες ή την παροχή ρεύματος, ή μη εξουσιοδοτημένη φυσική πρόσβαση και ζημία καθώς και παρεμβολές στις εγκαταστάσεις παροχής και επεξεργασίας πληροφοριών οντότητας της Ένωσης, που θα μπορούσαν να υπονομεύσουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, διαβιβάζονται, υποβάλλονται σε επεξεργασία ή είναι προσβάσιμα μέσω δικτυακών και πληροφοριακών συστημάτων.

---

[1] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972 και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80).

(7) Για τη διαχείριση των κινδύνων κυβερνοσφάλειας που εντοπίζονται βάσει του πλαισίου, κάθε οντότητα της Ένωσης θα πρέπει να λαμβάνει κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα. Τα μέτρα αυτά θα πρέπει να καλύπτουν τους τομείς και τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας που προβλέπονται στον παρόντα κανονισμό για την ενίσχυση της κυβερνοασφάλειας κάθε οντότητας της Ένωσης.

(8) Τα περιουσιακά στοιχεία και οι κίνδυνοι κυβερνοασφάλειας που προσδιορίζονται στο πλαίσιο, καθώς και τα συμπεράσματα που προκύπτουν από τακτικές αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας θα πρέπει να αντικατοπτρίζονται στο σχέδιο κυβερνοασφάλειας που καταρτίζει κάθε οντότητα της Ένωσης. Το σχέδιο κυβερνοασφάλειας θα πρέπει να περιλαμβάνει τα εγκεκριμένα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας.

(9) Δεδομένου ότι η διασφάλιση της κυβερνοασφάλειας αποτελεί συνεχή διαδικασία, η καταλληλότητα και η αποτελεσματικότητα των μέτρων που λαμβάνονται σύμφωνα με τον παρόντα κανονισμό θα πρέπει να αναθεωρούνται τακτικά υπό το πρίσμα των μεταβαλλόμενων κινδύνων κυβερνοασφάλειας, των περιουσιακών στοιχείων και του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας των οντοτήτων της Ένωσης. Το πλαίσιο θα πρέπει να επανεξετάζεται τακτικά και τουλάχιστον ανά τετραετία, ενώ το σχέδιο κυβερνοασφάλειας θα πρέπει να αναθεωρείται ανά διετία ή, συχνότερα όταν είναι αναγκαίο, μετά τις αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας ή μετά από οποιαδήποτε ουσιαστική επανεξέταση του πλαισίου.

(10) Τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας που εφαρμόζονται από οντότητες της Ένωσης θα πρέπει να περιλαμβάνουν πολιτικές που αποσκοπούν, όπου είναι δυνατόν, στη διαφάνεια του πηγαίου κώδικα, λαμβάνοντας υπόψη τις διασφαλίσεις για τα δικαιώματα τρίτων ή οντοτήτων της Ένωσης. Οι εν λόγω πολιτικές θα πρέπει να είναι αναλογικές προς τον κίνδυνο κυβερνοασφάλειας και αποσκοπούν στη διευκόλυνση της ανάλυσης των κυβερνοαπειλών, χωρίς να δημιουργούν υποχρεώσεις γνωστοποίησης ή δικαιώματα πρόσβασης σε κώδικα τρίτων πέραν των εφαρμοστέων συμβατικών όρων.

(11) Τα εργαλεία και οι εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα μπορούν να συμβάλουν στην ενίσχυση του βαθμού ανοικτότητας. Τα ανοικτά πρότυπα διευκολύνουν τη διαλειτουργικότητα μεταξύ των εργαλείων ασφάλειας, με οφέλη για την ασφάλεια των ενδιαφερόμενων μερών. Εάν χρησιμοποιούνται εργαλεία και εφαρμογές κυβερνοασφάλειας ανοικτού κώδικα, μπορεί να αξιοποιηθεί η ευρύτερη κοινότητα υπεύθυνων ανάπτυξης λογισμικού, και με τον τρόπο αυτό να καταστεί δυνατή η διαφοροποίηση των προμηθευτών. Ο ανοικτός κώδικας μπορεί να οδηγήσει σε διαφανέστερη διαδικασία επαλήθευσης των εργαλείων που σχετίζονται με την κυβερνοασφάλεια και σε μια διαδικασία εντοπισμού ευπαθειών σε επίπεδο κοινότητας. Συνεπώς, οι οντότητες της Ένωσης θα πρέπει να μπορούν να προωθήσουν τη χρήση λογισμικού ανοικτού κώδικα και ανοικτών προτύπων με την εφαρμογή πολιτικών που συνδέονται με τη χρήση ανοικτών δεδομένων και ανοικτού κώδικα στο πλαίσιο της ασφάλειας μέσω διαφάνειας.

(12) Οι διαφορές μεταξύ των οντοτήτων της Ένωσης απαιτούν ευελιξία κατά την εφαρμογή, του παρόντος κανονισμού. Τα μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας που προβλέπονται στον παρόντα κανονισμό δεν θα πρέπει να περιλαμβάνουν υποχρεώσεις που παρεμβαίνουν άμεσα στην άσκηση των αποστολών που έχουν ανατεθεί στις οντότητες της Ένωσης ή θίγουν τη θεσμική αυτονομία τους. Κατά συνέπεια, οι εν λόγω οντότητες θα πρέπει να θεσπίσουν τα δικά τους Πλαίσια και να εγκρίνουν τα δικά τους μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας και τα δικά τους σχέδια κυβερνοασφάλειας. Κατά την εφαρμογή των εν λόγω μέτρων, θα πρέπει να λαμβάνονται δεόντως υπόψη οι υφιστάμενες συνέργειες μεταξύ των οντοτήτων της Ένωσης, με σκοπό την ορθή διαχείριση των πόρων και τη βελτιστοποίηση του κόστους. Θα πρέπει επίσης να υπάρχει η δέουσα μέριμνα ώστε τα μέτρα να μην επηρεάζουν αρνητικά την αποτελεσματική ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των οντοτήτων της Ένωσης και μεταξύ των οντοτήτων της Ένωσης και ομολόγων τους στα κράτη μέλη.

(13) Προκειμένου να βελτιστοποιηθεί η χρήση των πόρων, ο παρών κανονισμός θα πρέπει να προβλέπει ότι δύο ή περισσότερες οντότητες της Ένωσης με παρόμοιες δομές έχουν τη δυνατότητα να συνεργάζονται όταν διενεργούν αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας για τις αντίστοιχες οντότητές τους.

(14) Για την αποφυγή δυσανάλογης οικονομικής και διοικητικής επιβάρυνσης των οντοτήτων της Ένωσης, οι απαιτήσεις σχετικά με τη διαχείριση κινδύνων κυβερνοασφάλειας θα πρέπει να είναι ανάλογες προς τον κίνδυνο κυβερνοασφάλειας που ενέχουν τα σχετικά συστήματα δικτύου και πληροφοριών, λαμβανομένων υπόψη των πλέον προηγμένων τεχνολογικών εξελίξεων όσον αφορά τα σχετικά μέτρα. Κάθε οντότητα της Ένωσης θα πρέπει να στοχεύει στη διάθεση επαρκούς ποσοστού του προϋπολογισμού του που αφορά την ΤΠΕ στη βελτίωση του επιπέδου κυβερνοασφάλειας. Μακροπρόθεσμα, θα πρέπει να επιδιωχθεί ενδεικτικός στόχος της τάξης τουλάχιστον του 10 %. Η αξιολόγηση του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας θα πρέπει να εκτιμά κατά πόσον οι δαπάνες της οντότητας της Ένωσης για την κυβερνοασφάλεια είναι ανάλογες προς τους κινδύνους κυβερνοασφάλειας που αντιμετωπίζει. Με την επιφύλαξη των κανόνων που αφορούν τον ετήσιο προϋπολογισμό της Ένωσης δυνάμει των Συνθηκών, στην πρότασή της για τον πρώτο ετήσιο προϋπολογισμό που θα εγκριθεί μετά την έναρξη ισχύος του παρόντος κανονισμού, η Επιτροπή θα πρέπει να λάβει υπόψη τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό κατά την αξιολόγηση των αναγκών προϋπολογισμού και στελέχωσης των οντοτήτων της Ένωσης, όπως αυτές προκύπτουν από τις εκτιμήσεις δαπανών τους.

(15) Για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, η κυβερνοασφάλεια θα πρέπει να τελεί υπό την εποπτεία του ανώτατου διοικητικού επιπέδου κάθε οντότητας της Ένωσης. Το ανώτατο διοικητικό επίπεδο της οντότητας της Ένωσης θα πρέπει να είναι υπεύθυνο για την εφαρμογή του παρόντος κανονισμού, μεταξύ άλλων για τη θέσπιση του πλαισίου, τη λήψη μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και την έγκριση του σχεδίου κυβερνοασφάλειας. Η δημιουργία νοοτροπίας κυβερνοασφάλειας, δηλαδή η καθημερινή πρακτική της κυβερνοασφάλειας, αποτελεί αναπόσπαστο μέρος του πλαισίου και των αντίστοιχων μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας σε όλες τις οντότητες της Ένωσης.

(16) Η ασφάλεια των δικτυακών και πληροφοριακών συστημάτων που χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ (ΔΠΕΕ) είναι ουσιαστικής σημασίας. Οι οντότητες της Ένωσης που χειρίζονται ΔΠΕΕ υποχρεούνται να εφαρμόζουν τα ολοκληρωμένα ρυθμιστικά πλαίσια που ισχύουν για την προστασία των εν λόγω πληροφοριών, συμπεριλαμβανομένων ειδικών ρυθμίσεων διακυβέρνησης, πολιτικών και διαδικασιών διαχείρισης κινδύνων. Είναι απαραίτητο τα δικτυακά και πληροφοριακά συστήματα που χειρίζονται ΔΠΕΕ να συμμορφώνονται με αυστηρότερα πρότυπα ασφαλείας από ό,τι τα μη διαβαθμισμένα δικτυακά και πληροφοριακά συστήματα. Με τον τρόπο αυτό, τα δικτυακά και πληροφοριακά συστήματα που χειρίζονται ΔΠΕΕ είναι πιο ανθεκτικά σε κυβερνοαπειλές και σχετικά περιστατικά. Κατά συνέπεια, μολονότι αναγνωρίζεται η ανάγκη για ένα κοινό πλαίσιο στον τομέα αυτό, ο παρών κανονισμός δεν θα πρέπει να εφαρμόζεται στα δικτυακά και πληροφοριακά συστήματα που χειρίζονται ΔΠΕΕ. Ωστόσο, εάν ζητηθεί ρητά από οντότητα της Ένωσης, η ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ (CERT-ΕΕ) θα πρέπει να είναι σε θέση να παρέχει συνδρομή στην εν λόγω οντότητα της Ένωσης σε σχέση με περιστατικά σε διαβαθμισμένα περιβάλλοντα ΤΠΕ.

(17) Οι οντότητες της Ένωσης θα πρέπει να αξιολογούν τους κινδύνους κυβερνοασφάλειας 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 κυβερνοασφάλειας θα πρέπει να εξειδικεύονται περαιτέρω σε κατευθυντήριες γραμμές ή συστάσεις που εκδίδονται από τη CERT-ΕΕ. Κατά τον καθορισμό μέτρων και κατευθυντήριων γραμμών, θα πρέπει να λαμβάνονται δεόντως υπόψη η εξέλιξη της τεχνολογίας και, κατά περίπτωση, τα οικεία ευρωπαϊκά και διεθνή πρότυπα, καθώς και η σχετική νομοθεσία και οι πολιτικές της Ένωσης, συμπεριλαμβανομένων των εκτιμήσεων κινδύνου κυβερνοασφάλειας και των συστάσεων που εκδίδονται από την Ομάδα Συνεργασίας που συστάθηκε σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555, όπως η συντονισμένη εκτίμηση κινδύνου της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G και η εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G. Επιπλέον, λαμβανομένων υπόψη του τοπίου κυβερνοαπειλών και της σημασίας της οικοδόμησης κυβερνοανθεκτικότητας για τις οντότητες της Ένωσης, θα μπορούσε να απαιτείται η πιστοποίηση σχετικών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, στο πλαίσιο ειδικών ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με το άρθρο 49 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1].

[1] 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).

(18) Τον Μάιο του 2011, οι γενικοί γραμματείς των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης αποφάσισαν να συγκροτήσουν μία ομάδα προ-διαμόρφωσης για την 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 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[1]. Ο παρών κανονισμός θα πρέπει να προβλέπει ένα ολοκληρωμένο σύνολο κανόνων σχετικά με την οργάνωση, τη λειτουργία και τη διαχείριση της CERT-ΕΕ. Οι διατάξεις του παρόντος κανονισμού υπερισχύουν των διατάξεων της διοργανικής συμφωνίας για την οργάνωση και τη λειτουργία της CERT-ΕΕ που συνήφθη τον Δεκέμβριο του 2017.

(19) Η CERT-ΕΕ θα πρέπει να μετονομαστεί σε Υπηρεσία Κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, αλλά θα πρέπει να διατηρήσει τη σύντομη ονομασία «CERT-ΕΕ» λόγω της αναγνωρισιμότητας της ονομασίας.

---

[1] Διακανονισμός μεταξύ του Ευρωπαϊκού Κοινοβουλίου, του Ευρωπαϊκού Συμβουλίου, του Συμβουλίου της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Επιτροπής, του Δικαστηρίου της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Κεντρικής Τράπεζας, του Ευρωπαϊκού Ελεγκτικού Συνεδρίου, της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης, της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής, της Ευρωπαϊκής Επιτροπής των Περιφερειών και της Ευρωπαϊκής Τράπεζας Επενδύσεων σχετικά με την οργάνωση και τη λειτουργία ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-ΕΕ) (ΕΕ C 12 της 13.1.2018, σ. 1).

(20) Επιπλέον της ανάθεσης περισσότερων καθηκόντων και διευρυμένου ρόλου στην CERT-ΕΕ, ο παρών κανονισμός δημιουργεί το Διοργανικό Συμβούλιο Κυβερνοασφάλειας (ΔΣΚ), προκειμένου να διευκολυνθεί η επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας μεταξύ των οντοτήτων της Ένωσης. Το ΔΣΚ θα πρέπει να έχει αποκλειστικό ρόλο στην παρακολούθηση και την υποστήριξη της εφαρμογής του παρόντος κανονισμού από τις οντότητες της Ένωσης, καθώς και στην εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από την CERT-ΕΕ και την παροχή στρατηγικών κατευθύνσεων στην CERT-ΕΕ. Το ΔΣΚ θα πρέπει, επομένως, να διασφαλίζει την εκπροσώπηση των θεσμικών οργάνων της Ένωσης και να περιλαμβάνει εκπροσώπους των λοιπών οργάνων και οργανισμών της Ένωσης μέσω του Δικτύου των Οργανισμών της ΕΕ (EUAN). Η οργάνωση και η λειτουργία του ΔΣΚ θα πρέπει να ρυθμίζονται περαιτέρω μέσω εσωτερικού κανονισμού, ο οποίος μπορεί να περιλαμβάνει περαιτέρω διευκρινίσεις για τις τακτικές συνεδριάσεις του ΔΣΚ, συμπεριλαμβανομένων των ετήσιων συναντήσεων σε πολιτικό επίπεδο, όπου εκπρόσωποι του ανώτατου διοικητικού επιπέδου κάθε μέλους του ΔΣΚ θα δίνουν τη δυνατότητα στο ΔΣΚ να πραγματοποιεί στρατηγικές συζητήσεις και θα του παρέχουν στρατηγική καθοδήγηση. Επιπλέον, το ΔΣΚ θα πρέπει να έχει τη δυνατότητα να διορίσει εκτελεστική επιτροπή για να το επικουρεί στο έργο του και να της αναθέσει ορισμένα από τα καθήκοντα και τις αρμοδιότητές του, ιδίως όσον αφορά καθήκοντα που απαιτούν ειδική εμπειρογνωσία των μελών της, για παράδειγμα την έγκριση του καταλόγου υπηρεσιών και τυχόν επακόλουθων επικαιροποιήσεών του, τις ρυθμίσεις για τις συμφωνίες σε επίπεδο υπηρεσιών, τις αξιολογήσεις των εγγράφων και των εκθέσεων που υποβάλλουν οι οντότητες της Ένωσης στο ΔΣΚ δυνάμει του παρόντος κανονισμού ή καθήκοντα που αφορούν την προετοιμασία των αποφάσεων που εκδίδει το ΔΣΚ σχετικά με μέτρα συμμόρφωσης, καθώς και την παρακολούθηση της εφαρμογής τους. Το ΔΣΚ θα πρέπει να θεσπίζει τον κανονισμό της εκτελεστικής επιτροπής, συμπεριλαμβανομένων των καθηκόντων και των εξουσιών της.

(21) Στόχος του ΔΣΚ είναι να στηρίξει τις οντότητες της Ένωσης ώστε να βελτιώσουν τη στάση τους στον τομέα της κυβερνοασφάλειας μέσω της εφαρμογής του παρόντος κανονισμού. Προκειμένου να στηρίξει τις οντότητες της Ένωσης, το ΔΣΚ θα πρέπει να παρέχει καθοδήγηση στον επικεφαλής της CERT-ΕΕ, να εγκρίνει πολυετή στρατηγική για τη βελτίωση του επιπέδου κυβερνοασφάλειας στις οντότητες της Ένωσης, να καθορίζει τη μεθοδολογία και άλλες πτυχές των εθελοντικών αξιολογήσεων από ομοτίμους και να διευκολύνει τη σύσταση άτυπης ομάδας τοπικών υπευθύνων κυβερνοασφάλειας, με την υποστήριξη του Οργανισμού της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια (ENISA), με στόχο την ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σε σχέση με την εφαρμογή του παρόντος κανονισμού.

(22) Προκειμένου να επιτευχθεί υψηλό επίπεδο κυβερνοασφάλειας σε όλες τις οντότητες της Ένωσης, τα συμφέροντα των λοιπών οργάνων και οργανισμών της Ένωσης που διαχειρίζονται το δικό τους περιβάλλον ΤΠΕ θα πρέπει να εκπροσωπούνται στο ΔΣΚ από τρεις εκπροσώπους που ορίζονται από το EUAN. Η ασφάλεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και, κατ' επέκταση, η κυβερνοασφάλειά τους αποτελεί ακρογωνιαίο λίθο της προστασίας των δεδομένων. Υπό το πρίσμα των συνεργειών μεταξύ της προστασίας των δεδομένων και της κυβερνοασφάλειας, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων θα πρέπει να εκπροσωπείται στο ΔΣΚ υπό την ιδιότητά του ως οντότητας της Ένωσης που υπόκειται στον παρόντα κανονισμό, με ειδική εμπειρογνωσία στον τομέα της προστασίας των δεδομένων, συμπεριλαμβανομένης της ασφάλειας των δικτύων ηλεκτρονικών επικοινωνιών. Λαμβανομένης υπόψη της σημασίας της καινοτομίας και της ανταγωνιστικότητας στην κυβερνοασφάλεια, το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας θα πρέπει να εκπροσωπείται στο ΔΣΚ. Δεδομένου του ρόλου του ENISA ως κέντρου εμπειρογνωσίας στον τομέα της κυβερνοασφάλειας και της στήριξης που παρέχει ο ENISA, και δεδομένης της σημασίας της κυβερνοασφάλειας των διαστημικών υποδομών και υπηρεσιών της Ένωσης, ο ENISA και ο Οργανισμός της Ευρωπαϊκής Ένωσης για το Διαστημικό Πρόγραμμα θα πρέπει να εκπροσωπούνται στο ΔΣΚ. Υπό το πρίσμα του ρόλου που ανατίθεται στην CERT-ΕΕ δυνάμει του παρόντος κανονισμού, ο επικεφαλής της CERT-ΕΕ θα πρέπει να προσκαλείται από τον πρόεδρο του ΔΣΚ σε όλες τις συνεδριάσεις του ΔΣΚ, εκτός εάν το ΔΣΚ συζητά θέματα που αφορούν άμεσα τον επικεφαλής της CERT-ΕΕ.

(23) Το ΔΣΚ θα πρέπει να παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, καθώς και την εφαρμογή όσον αφορά κατευθυντήριες γραμμές και συστάσεις, και εκκλήσεις για ανάληψη δράσης. Το ΔΣΚ θα πρέπει να υποστηρίζεται σε τεχνικά θέματα από τεχνικές συμβουλευτικές ομάδες οι οποίες θα συγκροτούνται κατά την κρίση του ΔΣΚ. Οι εν λόγω τεχνικές συμβουλευτικές ομάδες θα πρέπει να συνεργάζονται στενά με την CERT-ΕΕ, τις οντότητες της Ένωσης και άλλα ενδιαφερόμενα μέρη, κατά περίπτωση.

(24) Όταν το ΔΣΚ διαπιστώνει ότι μια οντότητα της Ένωσης δεν έχει εφαρμόσει αποτελεσματικά τον παρόντα κανονισμό ή τις κατευθυντήριες γραμμές, τις συστάσεις ή τις εκκλήσεις για ανάληψη δράσης που εκδίδονται δυνάμει αυτού, το ΔΣΚ θα πρέπει να είναι σε θέση, με την επιφύλαξη των εσωτερικών διαδικασιών της οικείας οντότητας της Ένωσης, να λαμβάνει μέτρα συμμόρφωσης. Το ΔΣΚ θα πρέπει να εφαρμόζει τα μέτρα συμμόρφωσης σταδιακά, δηλαδή θα πρέπει πρώτα να εγκρίνει το λιγότερο αυστηρό μέτρο, ήτοι την αιτιολογημένη γνώμη και, μόνον εάν είναι αναγκαίο, να εγκρίνει ολοένα και πιο αυστηρά μέτρα, καταλήγοντας στο πλέον αυστηρό μέτρο, ήτοι τη σύσταση για προσωρινή αναστολή των ροών δεδομένων προς την οικεία οντότητα της Ένωσης. Η σύσταση αυτή θα πρέπει να εφαρμόζεται μόνο σε εξαιρετικές περιπτώσεις μακροχρόνιων, εσκεμμένων ή σοβαρών παραβάσεων του παρόντος κανονισμού από την οικεία οντότητα της Ένωσης.

(25) Η αιτιολογημένη γνώμη αποτελεί το λιγότερο αυστηρό μέτρο συμμόρφωσης για την αντιμετώπιση των παρατηρούμενων κενών στην εφαρμογή του παρόντος κανονισμού. Το ΔΣΚ θα πρέπει να έχει τη δυνατότητα να δώσει συνέχεια σε μια αιτιολογημένη γνώμη, αρχικά με καθοδήγηση για να βοηθήσει την οντότητα της Ένωσης να διασφαλίσει ότι το πλαίσιό της, τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, το σχέδιο κυβερνοασφάλειας και η υποβολή εκθέσεων εκ μέρους της συμμορφώνονται με τον παρόντα κανονισμό, και έπειτα με προειδοποίηση για την αντιμετώπιση των ελλείψεων που εντοπίστηκαν στην οντότητα της Ένωσης εντός καθορισμένου χρονικού διαστήματος. Εάν οι ελλείψεις που προσδιορίζονται στην προειδοποίηση δεν έχουν αντιμετωπιστεί επαρκώς, το ΔΣΚ θα πρέπει να έχει τη δυνατότητα να εκδώσει αιτιολογημένη κοινοποίηση.

(26) Το ΔΣΚ θα πρέπει να έχει τη δυνατότητα να προβεί σε σύσταση για τη διενέργεια ελέγχου σε οντότητα της Ένωσης. Για τον σκοπό αυτόν η οντότητα της Ένωσης θα πρέπει να μπορεί να απευθυνθεί στη μονάδα εσωτερικού ελέγχου της. Το ΔΣΚ θα πρέπει επίσης να έχει τη δυνατότητα να ζητήσει τη διενέργεια ελέγχου από τρίτο φορέα παροχής υπηρεσιών ελέγχου, μεταξύ άλλων από αμοιβαία αποδεκτό πάροχο υπηρεσιών του ιδιωτικού τομέα.

(27) Σε εξαιρετικές περιπτώσεις μακροχρόνιων, εσκεμμένων, επαναλαμβανόμενων ή σοβαρών παραβάσεων του παρόντος κανονισμού από οντότητα της Ένωσης, το ΔΣΚ θα πρέπει να έχει τη δυνατότητα να συνιστά σε όλα τα κράτη μέλη και τις οντότητες της Ένωσης, ως έσχατη λύση, την προσωρινή αναστολή των ροών δεδομένων προς την οντότητα της Ένωσης, η οποία θα ισχύει έως ότου η οντότητα της Ένωσης σταματήσει την παράβαση. Η σύσταση αυτή θα πρέπει να κοινοποιείται μέσω κατάλληλων και ασφαλών διαύλων επικοινωνίας.

(28) Για να διασφαλιστεί η ορθή εφαρμογή του παρόντος κανονισμού, το ΔΣΚ θα πρέπει —εάν κρίνει ότι η διαρκής παράβαση του παρόντος κανονισμού από οντότητα της Ένωσης προκλήθηκε άμεσα από πράξεις ή παραλείψεις μέλους του προσωπικού της, μεταξύ άλλων και στο ανώτατο διοικητικό επίπεδο— να ζητήσει από την οικεία οντότητα της Ένωσης να λάβει τα κατάλληλα μέτρα, μεταξύ άλλων ζητώντας της να εξετάσει το ενδεχόμενο λήψης μέτρων πειθαρχικού χαρακτήρα, σύμφωνα με τους κανόνες και τις διαδικασίες που ορίζονται στον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων της Ευρωπαϊκής Ένωσης και στο καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ένωσης, όπως καθορίζονται με τον κανονισμό (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 του Συμβουλίου[1] («κανονισμός υπηρεσιακής κατάστασης»), και οποιουσδήποτε άλλους εφαρμοστέους κανόνες και διαδικασίες.

(29) Η CERT-ΕΕ θα πρέπει να συμβάλλει στην ασφάλεια του περιβάλλοντος ΤΠΕ όλων των οντοτήτων της Ένωσης. Όταν εξετάζει το ενδεχόμενο να παράσχει τεχνικές συμβουλές ή στοιχεία για συναφή ζητήματα πολιτικής κατόπιν αιτήματος οντότητας της Ένωσης, η CERT-ΕΕ θα πρέπει να βεβαιώνεται ότι αυτό δεν αποτελεί εμπόδιο για την εκτέλεση των άλλων καθηκόντων που της ανατίθενται δυνάμει του παρόντος κανονισμού. Η CERT-ΕΕ θα πρέπει να ενεργεί εκ μέρους των οντοτήτων της Ένωσης ως το αντίστοιχο όργανο του συντονιστή που ορίζεται για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών σύμφωνα με το άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555.

---

[1] Κανονισμός (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 του Συμβουλίου, της 29ης Φεβρουαρίου 1968, περί καθορισμού του κανονισμού υπηρεσιακής καταστάσεως των υπαλλήλων και του καθεστώτος που εφαρμόζεται επί του λοιπού προσωπικού των Ευρωπαϊκών Κοινοτήτων και περί θεσπίσεως ειδικών μέτρων προσωρινώς εφαρμοστέων στους υπαλλήλους της Επιτροπής (ΕΕ L 56 της 4.3.1968, σ. 1).

(30) Η CERT-ΕΕ θα πρέπει να στηρίξει την εφαρμογή μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας μέσω προτάσεων για κατευθυντήριες γραμμές και συστάσεις προς το ΔΣΚ ή μέσω της έκδοσης εκκλήσεων για ανάληψη δράσης. Οι εν λόγω κατευθυντήριες γραμμές και συστάσεις θα πρέπει να εγκρίνονται από το ΔΣΚ. 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 οι οντότητες της Ένωσης εντός καθορισμένου χρονικού πλαισίου. Το ΔΣΚ θα πρέπει να εκδίδει εντολή προς την CERT-ΕΕ για την έκδοση, την ανάκληση ή την τροποποίηση πρότασης για κατευθυντήριες γραμμές ή για σύσταση, ή έκκλησης για ανάληψη δράσης.

(31) Η CERT-ΕΕ θα πρέπει επίσης να εκπληρώνει τον ρόλο που προβλέπεται στην οδηγία (ΕΕ) 2022/2555 όσον αφορά τη συνεργασία και την ανταλλαγή πληροφοριών με το δίκτυο των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές («CSIRT») που συστάθηκε σύμφωνα με το άρθρο 15 της εν λόγω οδηγίας. Επιπλέον, σύμφωνα με τη σύσταση της Επιτροπής (ΕΕ) 2017/1584[1], 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 Ένωση, η CERT-ΕΕ θα πρέπει να ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά με τους ομολόγους της στα κράτη μέλη. Η CERT-ΕΕ θα πρέπει επίσης να συνεργάζεται με άλλους ομολόγους από τον δημόσιο και τον ιδιωτικό τομέα, συμπεριλαμβανομένου του Οργανισμού Βορειοατλαντικού Συμφώνου, με την επιφύλαξη προηγούμενης έγκρισης από το ΔΣΚ.

[1] 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).

(32) Για τη στήριξη της επιχειρησιακής κυβερνοασφάλειας, η CERT-ΕΕ θα πρέπει να χρησιμοποιεί τη διαθέσιμη εμπειρογνωσία του ENISA μέσω διαρθρωμένης συνεργασίας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2019/881. 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 ENISA όσον αφορά την ανάλυση κυβερνοαπειλών και να του κοινοποιεί την έκθεσή της για το τοπίο των απειλών σε τακτική βάση.

(33) Η CERT-ΕΕ θα πρέπει να έχει τη δυνατότητα να συνεργάζεται και να ανταλλάσσει πληροφορίες με σχετικές κοινότητες κυβερνοασφάλειας στην Ένωση και τα κράτη μέλη της, 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.

(34) Δεδομένου ότι οι υπηρεσίες και τα καθήκοντα της CERT-ΕΕ είναι προς το συμφέρον των οντοτήτων της Ένωσης, κάθε οντότητα της Ένωσης με δαπάνες ΤΠΕ θα πρέπει να συνεισφέρει δίκαιο μερίδιο στις εν λόγω υπηρεσίες και καθήκοντα. Οι συνεισφορές αυτές δεν θίγουν τη δημοσιονομική αυτονομία των οντοτήτων της Ένωσης.

(35) Πολλές κυβερνοεπιθέσεις αποτελούν μέρος ευρύτερων εκστρατειών που έχουν ως στόχο ομάδες οντοτήτων της Ένωσης ή κοινότητες ενδιαφέροντος που περιλαμβάνουν οντότητες της Ένωσης. Για να καταστούν δυνατά ο προδραστικός εντοπισμός, η αντιμετώπιση περιστατικών ή η εφαρμογή μέτρων μετριασμού και η ανάκαμψη από περιστατικά, οι οντότητες της Ένωσης θα πρέπει να έχουν τη δυνατότητα κοινοποιούν στην CERT-ΕΕ περιστατικά, κυβερνοαπειλές, ευπάθειες και παρ' ολίγον περιστατικά και να ανταλλάσσουν κατάλληλες τεχνικές λεπτομέρειες που καθιστούν δυνατό τον εντοπισμό ή τον μετριασμό παρόμοιων περιστατικών, κυβερνοαπειλών, ευπαθειών και παρ' ολίγον περιστατικών, καθώς και την αντιμετώπισή τους, σε άλλες οντότητες της Ένωσης. Ακολουθώντας την ίδια προσέγγιση όπως στην οδηγία (ΕΕ) 2022/2555, οι οντότητες της Ένωσης θα πρέπει να υποχρεούνται να υποβάλουν έγκαιρη προειδοποίηση στην CERT-ΕΕ εντός 24 ωρών από τη στιγμή που αντιλαμβάνονται σημαντικό περιστατικό. Η εν λόγω ανταλλαγή πληροφοριών θα πρέπει να παρέχει στην CERT-ΕΕ τη δυνατότητα να διαδίδει τις πληροφορίες σε άλλες οντότητες της Ένωσης, καθώς και σε κατάλληλους ομολόγους τους, ώστε να συμβάλλει στην προστασία των περιβαλλόντων ΤΠΕ των οντοτήτων της Ένωσης και των περιβαλλόντων ΤΠΕ των ομολόγων των οντοτήτων της Ένωσης από παρόμοια περιστατικά.

(36) Ο παρών κανονισμός καθορίζει μια προσέγγιση πολλαπλών σταδίων για την αναφορά σημαντικών περιστατικών, προκειμένου να επιτευχθεί η σωστή ισορροπία μεταξύ, αφενός, της ταχείας αναφοράς που συμβάλλει στον μετριασμό της πιθανής εξάπλωσης σημαντικών περιστατικών και επιτρέπει στις οντότητες της Ένωσης να αναζητήσουν υποστήριξη, και, αφετέρου της εμπεριστατωμένης αναφοράς που αντλεί πολύτιμα διδάγματα από μεμονωμένα περιστατικά και βελτιώνει με την πάροδο του χρόνου την κυβερνοανθεκτικότητα των επιμέρους οντοτήτων της Ένωσης και συμβάλλει στην ενίσχυση της συνολικής στάσης τους στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτό, ο παρών κανονισμός θα πρέπει να περιλαμβάνει την αναφορά περιστατικών τα οποία, βάσει αρχικής αξιολόγησης που διενεργείται από την οικεία οντότητα της Ένωσης, θα μπορούσαν να προκαλέσουν σοβαρή λειτουργική διατάραξη ή οικονομική ζημία στην οικεία οντότητα της Ένωσης ή να επηρεάσουν άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία. Αυτή η αρχική αξιολόγηση θα πρέπει να λαμβάνει υπόψη, μεταξύ άλλων, τα θιγόμενα δικτυακά και πληροφοριακά συστήματα, ιδίως τη σημασία τους για τη λειτουργία της οντότητας της Ένωσης, τη σοβαρότητα και τα τεχνικά χαρακτηριστικά μιας κυβερνοαπειλής και τυχόν υποκείμενες ευπάθειες που αποτελούν αντικείμενο εκμετάλλευσης, καθώς και την πείρα της οντότητας της Ένωσης από παρόμοια περιστατικά. Δείκτες όπως ο βαθμός στον οποίο θίγεται η λειτουργία της οντότητας της Ένωσης, η διάρκεια ενός περιστατικού ή ο αριθμός των θιγόμενων φυσικών ή νομικών προσώπων θα μπορούσαν να διαδραματίσουν σημαντικό ρόλο στον χαρακτηρισμό της λειτουργικής διατάραξης ως σοβαρής.

(37) Καθώς οι υποδομές και τα δικτυακά και πληροφοριακά συστήματα της σχετικής οντότητας της Ένωσης και του κράτους μέλους στο οποίο βρίσκεται η εν λόγω οντότητα της Ένωσης είναι διασυνδεδεμένα, η χωρίς αδικαιολόγητη καθυστέρηση ενημέρωση του εν λόγω κράτους μέλους για σημαντικό περιστατικό εντός της εν λόγω οντότητας της Ένωσης είναι καίριας σημασίας. Για τον σκοπό αυτό, η θιγόμενη οντότητα της Ένωσης θα πρέπει να ενημερώνει κάθε σχετικό ομόλογό της στα κράτη μέλη που έχει οριστεί ή συσταθεί σύμφωνα με τα άρθρα 8 και 10 της οδηγίας (ΕΕ) 2022/2555 σχετικά με την εμφάνιση σημαντικού περιστατικού για το οποίο υποβάλλει έκθεση στην CERT-ΕΕ. Όταν η CERT-ΕΕ αντιλαμβάνεται σημαντικό περιστατικό που λαμβάνει χώρα εντός κράτους μέλους, θα πρέπει να ενημερώνει τον αντίστοιχο ομόλογο στο εν λόγω κράτος μέλος.

(38) Θα πρέπει να εφαρμοστεί μηχανισμός για τη διασφάλιση της αποτελεσματικής ανταλλαγής πληροφοριών, του συντονισμού και της συνεργασίας των οντοτήτων της Ένωσης σε περίπτωση σημαντικών περιστατικών, συμπεριλαμβανομένου σαφούς προσδιορισμού των ρόλων και των αρμοδιοτήτων των εμπλεκόμενων οντοτήτων της Ένωσης. Ο εκπρόσωπος της Επιτροπής στο ΔΣΚ θα πρέπει, με την επιφύλαξη του σχεδίου διαχείρισης κρίσεων στον κυβερνοχώρο, να αποτελεί το σημείο επαφής που θα διευκολύνει το ΔΣΚ να ανταλλάσσει σχετικές πληροφορίες όσον αφορά σοβαρά συμβάντα με το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe), ως συμβολή στην κοινή επίγνωση της κατάστασης. Ο ρόλος του εκπροσώπου της Επιτροπής στο ΔΣΚ ως σημείου επαφής δεν θα πρέπει να θίγει τον χωριστό και διακριτό ρόλο της Επιτροπής στο EU-CyCLONe σύμφωνα με το άρθρο 16 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555.

(39) Ο κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1] εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε να πραγματοποιείται σε σχέση με μέτρα που λαμβάνονται στο πλαίσιο της διαχείρισης κινδύνων κυβερνοασφάλειας, του χειρισμού ευπαθειών και περιστατικών, της ανταλλαγής πληροφοριών σχετικά με περιστατικά, κυβερνοαπειλές και ευπάθειες, και του συντονισμού και της συνεργασίας για την αντιμετώπιση περιστατικών. Τα μέτρα αυτά θα μπορούσαν να απαιτούν την επεξεργασία ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως διευθύνσεις IP, ενιαίοι εντοπιστές πόρων (URL), ονόματα τομέα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, οργανωτικοί ρόλοι του υποκειμένου των δεδομένων, χρονοσφραγίδες, θέματα μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ονόματα αρχείων. Όλα τα μέτρα που λαμβάνονται δυνάμει του παρόντος κανονισμού θα πρέπει να συμμορφώνονται με το πλαίσιο προστασίας των δεδομένων και της ιδιωτικότητας, και οι οντότητες της Ένωσης, η CERT-ΕΕ και, κατά περίπτωση, το ΔΣΚ θα πρέπει να εφαρμόζουν όλες τις σχετικές τεχνικές και οργανωτικές διασφαλίσεις για να εξασφαλίζουν τη συμμόρφωση αυτή με υπεύθυνο τρόπο.

(40) Με τον παρόντα κανονισμό θεσπίζεται η νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από οντότητες της Ένωσης, την CERT-ΕΕ και, κατά περίπτωση, το ΔΣΚ, για τους σκοπούς της εκτέλεσης των καθηκόντων τους και της εκπλήρωσης των υποχρεώσεών τους δυνάμει του παρόντος κανονισμού, σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο β) του κανονισμού (ΕΕ) 2018/1725. Η CERT-ΕΕ μπορεί να ενεργεί ως εκτελών την επεξεργασία ή υπεύθυνος επεξεργασίας ανάλογα με το καθήκον που εκτελεί σύμφωνα με τον κανονισμό (ΕΕ) 2018/1725.

---

[1] 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).

(41) Σε ορισμένες περιπτώσεις, ενδέχεται οι οντότητες της Ένωσης και η CERT-ΕΕ να πρέπει να επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως αυτές αναφέρονται στο άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725, προκειμένου να συμμορφωθούν με την υποχρέωσή τους, δυνάμει του παρόντος κανονισμού, να διασφαλίζουν υψηλό επίπεδο κυβερνοασφάλειας, και συγκεκριμένα στο πλαίσιο του χειρισμού ευπαθειών και περιστατικών. Με τον παρόντα κανονισμό θεσπίζεται η νομική βάση για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα από οντότητες της Ένωσης και την CERT-ΕΕ σύμφωνα με το άρθρο 10 παράγραφος 2 στοιχείο ζ) του κανονισμού (ΕΕ) 2018/1725. Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού θα πρέπει να είναι αυστηρά αναλογική προς τον επιδιωκόμενο στόχο. Με την επιφύλαξη των προϋποθέσεων που ορίζονται στο άρθρο 10 παράγραφος 2 στοιχείο ζ) του εν λόγω κανονισμού, οι οντότητες της Ένωσης και η CERT-ΕΕ θα πρέπει να έχουν τη δυνατότητα να επεξεργάζονται τα εν λόγω δεδομένα μόνο στον βαθμό που είναι αναγκαίο και όπου προβλέπεται ρητά στον παρόντα κανονισμό. Κατά την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, οι οντότητες της Ένωσης και η CERT-ΕΕ θα πρέπει να σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και να προβλέπουν κατάλληλα και ειδικά μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων των υποκειμένων των δεδομένων.

(42) Σύμφωνα με το άρθρο 33 του κανονισμού (ΕΕ) 2018/1725, οι οντότητες της Ένωσης και η CERT-ΕΕ θα πρέπει, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας των δεδομένων προσωπικού χαρακτήρα, όπως η παροχή περιορισμένων δικαιωμάτων πρόσβασης με βάση την ανάγκη γνώσης, η εφαρμογή των αρχών της διαδρομής ελέγχου, η έγκριση αλυσίδας επιτήρησης, η αποθήκευση των αδρανών δεδομένων σε ελεγχόμενο και ελέγξιμο περιβάλλον, τυποποιημένες επιχειρησιακές διαδικασίες και μέτρα προστασίας της ιδιωτικότητας, όπως η ψευδωνυμοποίηση ή η κρυπτογράφηση. Τα εν λόγω μέτρα δεν θα πρέπει να εφαρμόζονται κατά τρόπο που να επηρεάζει τους σκοπούς του χειρισμού περιστατικών και της ακεραιότητας των αποδεικτικών στοιχείων. Όταν μια οντότητα της Ένωσης ή η CERT-ΕΕ διαβιβάζει δεδομένα προσωπικού χαρακτήρα που σχετίζονται με περιστατικό, συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, σε ομόλογο ή εταίρο για τους σκοπούς του παρόντος κανονισμού, οι εν λόγω διαβιβάσεις θα πρέπει να συμμορφώνονται με τον κανονισμό (ΕΕ) 2018/1725. Όταν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα διαβιβάζονται σε τρίτο μέρος, οι οντότητες της Ένωσης και η CERT-ΕΕ θα πρέπει να διασφαλίζουν ότι το τρίτο μέρος εφαρμόζει μέτρα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα σε επίπεδο ισοδύναμο με αυτό του κανονισμού (ΕΕ) 2018/1725.

(43) Τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για τους σκοπούς του παρόντος κανονισμού θα πρέπει να διατηρούνται μόνο για όσο διάστημα είναι αναγκαίο σύμφωνα με τον κανονισμό (ΕΕ) 2018/1725. Όταν οι οντότητες της Ένωσης και, κατά περίπτωση, η CERT-ΕΕ ενεργούν ως υπεύθυνοι επεξεργασίας, θα πρέπει να ορίζουν περιόδους διατήρησης οι οποίες περιορίζονται στο διάστημα που είναι αναγκαίο για την επίτευξη των καθορισμένων σκοπών. Ιδίως σε σχέση με τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται για τον χειρισμό περιστατικών, οι οντότητες της Ένωσης και η CERT-ΕΕ θα πρέπει να κάνουν διάκριση μεταξύ, αφενός, των δεδομένων προσωπικού χαρακτήρα που συλλέγονται για τον εντοπισμό κυβερνοαπειλής στα δικά τους περιβάλλοντα ΤΠΕ με σκοπό την πρόληψη περιστατικού και, αφετέρου, των δεδομένων προσωπικού χαρακτήρα που συλλέγονται για τον μετριασμό ή την αντιμετώπιση περιστατικού και την ανάκαμψη από περιστατικό. Για τον εντοπισμό κυβερνοαπειλής, είναι σημαντικό να λαμβάνεται υπόψη ο χρόνος κατά τον οποίο ένας παράγοντας απειλής μπορεί να παραμένει αφανής σε ένα σύστημα. Για τον μετριασμό ή την αντιμετώπιση περιστατικού και την ανάκαμψη από περιστατικό, είναι σημαντικό να εξετάζεται κατά πόσον τα δεδομένα προσωπικού χαρακτήρα είναι αναγκαία για τον εντοπισμό και τον χειρισμό επαναλαμβανόμενου περιστατικού ή περιστατικού παρόμοιου χαρακτήρα με το οποίο θα μπορούσε να αποδειχθεί συσχέτιση.

(44) Ο χειρισμός πληροφοριών από τις οντότητες της Ένωσης και την CERT-ΕΕ θα πρέπει να συνάδει με τους ισχύοντες κανόνες για την ασφάλεια των πληροφοριών. Η συμπερίληψη της ασφάλειας των ανθρώπινων πόρων ως μέτρου διαχείρισης κινδύνων κυβερνοασφάλειας θα πρέπει επίσης να συμμορφώνεται με τους ισχύοντες κανόνες.

(45) Για τον σκοπό της ανταλλαγής πληροφοριών, χρησιμοποιούνται εμφανείς σημάνσεις που υποδεικνύουν ότι οι αποδέκτες των πληροφοριών πρέπει να τηρούν ορισμένα όρια κατά την ανταλλαγή πληροφοριών βάσει, ιδίως, συμφωνιών τήρησης του απορρήτου ή άτυπων συμφωνιών τήρησης του απορρήτου, όπως το πρωτόκολλο φωτεινού σηματοδότη (Traffic Light Protocol, TLP) ή άλλες σαφείς ενδείξεις από την πηγή. Το πρωτόκολλο φωτεινού σηματοδότη πρέπει να νοείται ως μέσο που επιτρέπει την παροχή πληροφοριών σχετικά με τυχόν περιορισμούς στην περαιτέρω διάδοση πληροφοριών. Χρησιμοποιείται σε όλες σχεδόν τις ομάδες CSIRT και σε ορισμένα κέντρα ανάλυσης και ανταλλαγής πληροφοριών.

(46) Ο παρών κανονισμός θα πρέπει να αξιολογείται σε τακτική βάση υπό το πρίσμα των μελλοντικών διαπραγματεύσεων για πολυετή δημοσιονομικά πλαίσια, ώστε να είναι δυνατή η λήψη περαιτέρω αποφάσεων όσον αφορά τον λειτουργικό και θεσμικό ρόλο της CERT-ΕΕ, συμπεριλαμβανομένης της πιθανής σύστασης της CERT-ΕΕ ως γραφείου της Ένωσης.

(47) Το ΔΣΚ, με τη συνδρομή της CERT-ΕΕ, θα πρέπει να επανεξετάζει και να αξιολογεί την εφαρμογή του παρόντος κανονισμού και να υποβάλλει έκθεση με τα πορίσματά του στην Επιτροπή. Με βάση αυτά τα στοιχεία, η Επιτροπή θα πρέπει να υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών. Η εν λόγω έκθεση, με τη συμβολή του ΔΣΚ, θα πρέπει να αξιολογεί τη σκοπιμότητα της συμπερίληψης δικτυακών και πληροφοριακών συστημάτων τα οποία χειρίζονται ΔΠΕΕ που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, ιδίως ελλείψει κοινών κανόνων ασφάλειας πληροφοριών για τις οντότητες της Ένωσης.

(48) Σύμφωνα με την αρχή της αναλογικότητας, είναι αναγκαίο και πρόσφορο προκειμένου να υλοποιηθεί ο θεμελιώδης στόχος της επίτευξης υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός των οντοτήτων της Ένωσης, να καθοριστούν κανόνες σχετικά με την κυβερνοασφάλεια για τις οντότητες της Ένωσης. Ο παρών κανονισμός δεν υπερβαίνει τα απαιτούμενα για την επίτευξη του επιδιωκόμενου στόχου, σύμφωνα με το άρθρο 5 παράγραφος 4 της Συνθήκης για την Ευρωπαϊκή Ένωση.

(49) Ο παρών κανονισμός αντικατοπτρίζει το γεγονός ότι οι οντότητες της Ένωσης διαφέρουν ως προς το μέγεθος και τις δυνατότητες, μεταξύ άλλων όσον αφορά τους οικονομικούς και ανθρώπινους πόρους.

(50) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725, η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 17 Μαΐου 2022[1],

ΕΞΕΔΩΣΑΝ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

[1] ΕΕ C 258 της 5.7.2022, σ. 10.

Κεφάλαιο I
Γενικές διατάξεις

Άρθρο 1

Αντικείμενο

Ο παρών κανονισμός θεσπίζει μέτρα που αποσκοπούν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός των οντοτήτων της Ένωσης όσον αφορά:

α) τη θέσπιση από κάθε οντότητα της Ένωσης εσωτερικού πλαισίου διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας, βάσει του άρθρου 6·

β) τη διαχείριση κινδύνων κυβερνοασφάλειας, την υποβολή εκθέσεων και την ανταλλαγή πληροφοριών·

γ) την οργάνωση, τη λειτουργία και τη διαχείριση του διοργανικού συμβουλίου κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10, καθώς και την οργάνωση, τη λειτουργία και τη διαχείριση της Υπηρεσίας Κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (CERT-EE)·

δ) την παρακολούθηση της εφαρμογής του παρόντος κανονισμού.

Άρθρο 2

Πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται στις οντότητες της Ένωσης, στο διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10 και στην CERT-ΕΕ.

2. Ο παρών κανονισμός εφαρμόζεται με την επιφύλαξη της θεσμικής αυτονομίας σύμφωνα με τις Συνθήκες.

3. Με εξαίρεση το άρθρο 13 παράγραφος 8, ο παρών κανονισμός δεν εφαρμόζεται στα δικτυακά και πληροφοριακά συστήματα που χειρίζονται διαβαθμισμένες πληροφορίες της ΕΕ (ΔΠΕΕ).

Άρθρο 3

Ορισμοί

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

1) «οντότητες 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 (ΣΛΕΕ) ή τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, ή δυνάμει των Συνθηκών αυτών·

2) «δικτυακό και πληροφοριακό σύστημα»: το δικτυακό και πληροφοριακό σύστημα όπως ορίζεται στο άρθρο 6 σημείο 1) της οδηγίας (ΕΕ) 2022/2555·

3) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ασφάλεια συστημάτων δικτύου και πληροφοριών όπως ορίζεται στο άρθρο 6 σημείο 2) της οδηγίας (ΕΕ) 2022/2555·

4) «κυβερνοασφάλεια»: η κυβερνοασφάλεια όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) 2019/881·

5) «ανώτατο διοικητικό επίπεδο»: διοικητικό στέλεχος, όργανο διοίκησης ή όργανο συντονισμού και εποπτείας αρμόδιο για τη λειτουργία οντότητας της Ένωσης, στο ανώτερο διοικητικό επίπεδο, με εντολή να εκδίδει ή να εγκρίνει αποφάσεις σύμφωνα με τις ρυθμίσεις διακυβέρνησης υψηλού επιπέδου της εν λόγω οντότητας της Ένωσης και με την επιφύλαξη των τυπικών αρμοδιοτήτων άλλων επιπέδων διοίκησης όσον αφορά τη συμμόρφωση και τη διαχείριση κινδύνων κυβερνοασφάλειας στους αντίστοιχους τομείς αρμοδιότητάς τους·

6) «παρ' ολίγον περιστατικό»: το παρ' ολίγον περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 5) της οδηγίας (ΕΕ) 2022/2555·

7) «περιστατικό»: το περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 6) της οδηγίας (ΕΕ) 2022/2555·

8) «σοβαρό περιστατικό»: κάθε περιστατικό που προκαλεί διαταραχή η οποία υπερβαίνει την ικανότητα μιας οντότητας της Ένωσης και της CERT-ΕΕ να ανταποκριθεί σε αυτήν ή που έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο οντότητες της Ένωσης·

9) «περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας»: το περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας όπως ορίζεται στο άρθρο 6 σημείο 7) της οδηγίας (ΕΕ) 2022/2555·

10) «χειρισμός περιστατικών»: ο χειρισμός περιστατικών όπως ορίζεται στο άρθρο 6 σημείο 8) της οδηγίας (ΕΕ) 2022/2555·

11) «κυβερνοαπειλή»: η κυβερνοαπειλή όπως ορίζεται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/881·

12) «σημαντική κυβερνοαπειλή»: η σημαντική κυβερνοαπειλή όπως ορίζεται στο άρθρο 6 σημείο 11) της οδηγίας (ΕΕ) 2022/2555·

13) «ευπάθεια»: η ευπάθεια όπως ορίζεται στο άρθρο 6 σημείο 15 της οδηγίας (ΕΕ) 2022/2555·

14) «κίνδυνος κυβερνοασφάλειας»: ο κίνδυνος όπως ορίζεται στο άρθρο 6 σημείο 9) της οδηγίας (ΕΕ) 2022/2555·

15) «υπηρεσία υπολογιστικού νέφους»: η υπηρεσία υπολογιστικού νέφους όπως περιγράφεται στο άρθρο 6 σημείο 30) της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 4

Επεξεργασία δεδομένων προσωπικού χαρακτήρα

1. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού από την CERT-ΕΕ, το διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10, και τις οντότητες της Ένωσης, διενεργείται σύμφωνα με τον κανονισμό (ΕΕ) 2018/1725.

2. Όταν εκτελούν καθήκοντα ή εκπληρώνουν υποχρεώσεις σύμφωνα με τον παρόντα κανονισμό, η CERT-ΕΕ, το διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10 και οι οντότητες της Ένωσης επεξεργάζονται και ανταλλάσσουν δεδομένα προσωπικού χαρακτήρα μόνο στον βαθμό που είναι αναγκαίο και με αποκλειστικό σκοπό την εκτέλεση των εν λόγω καθηκόντων ή την εκπλήρωση των εν λόγω υποχρεώσεων.

3. Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως αναφέρεται στο άρθρο 10 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725, θεωρείται απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος σύμφωνα με το άρθρο 10 παράγραφος 2 στοιχείο ζ) του εν λόγω κανονισμού. Τα εν λόγω δεδομένα μπορούν να υποβάλλονται σε επεξεργασία μόνο στον βαθμό που απαιτείται για την εφαρμογή των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας που αναφέρονται στα άρθρα 6 και 8, για την παροχή υπηρεσιών από την CERT-ΕΕ σύμφωνα με το άρθρο 13, για την ανταλλαγή πληροφοριών σχετικά με συγκεκριμένα περιστατικά σύμφωνα με το άρθρο 17 παράγραφος 3 και το άρθρο 18 παράγραφος 3, για την ανταλλαγή πληροφοριών σύμφωνα με το άρθρο 20, για τις υποχρεώσεις υποβολής εκθέσεων σύμφωνα με το άρθρο 21, για τον συντονισμό της αντιμετώπισης περιστατικών και τη σχετική συνεργασία σύμφωνα με το άρθρο 22 και για τη διαχείριση σοβαρών περιστατικών σύμφωνα με το άρθρο 23 του παρόντος κανονισμού. Οι οντότητες της Ένωσης και η CERT-ΕΕ, όταν ενεργούν ως υπεύθυνοι επεξεργασίας δεδομένων, εφαρμόζουν τεχνικά μέτρα για την πρόληψη της επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς και προβλέπουν κατάλληλα και ειδικά μέτρα προκειμένου να διασφαλίζονται τα θεμελιώδη δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων.

Κεφάλαιο ΙΙ

Μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας

Άρθρο 5

Εφαρμογή των μέτρων

1. Έως τις … [οκτώ μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], το διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10, κατόπιν διαβούλευσης με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και αφού λάβει καθοδήγηση από την CERT-EE, εκδίδει κατευθυντήριες γραμμές προς τις οντότητες της Ένωσης με σκοπό τη διενέργεια αρχικής επανεξέτασης της κυβερνοασφάλειας και τη θέσπιση του εσωτερικού πλαισίου διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας σύμφωνα με το άρθρο 6, τη διενέργεια αξιολογήσεων του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 7, τη λήψη μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας σύμφωνα με το άρθρο 8 και την έγκριση του σχεδίου κυβερνοασφάλειας σύμφωνα με το άρθρο 9.

2. Κατά την εφαρμογή των άρθρων 6 έως 9, οι οντότητες της Ένωσης λαμβάνουν υπόψη τις κατευθυντήριες γραμμές που αναφέρονται στην παράγραφο 1 του παρόντος άρθρου, καθώς και τις σχετικές κατευθυντήριες γραμμές και συστάσεις που εκδίδονται σύμφωνα με τα άρθρα 11 και 14.

Άρθρο 6

Πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων

1. Έως τις … [15 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], κάθε οντότητα της Ένωσης, μετά τη διενέργεια αρχικής επανεξέτασης της κυβερνοασφάλειας, π.χ. μέσω ελέγχου, θεσπίζει εσωτερικό πλαίσιο διαχείρισης, διακυβέρνησης και ελέγχου κινδύνων κυβερνοασφάλειας («το πλαίσιο»). Η θέσπιση του πλαισίου εποπτεύεται και τελεί υπό την ευθύνη του ανώτατου διοικητικού επιπέδου της οντότητας της Ένωσης.

2. Το πλαίσιο καλύπτει ολόκληρο το μη διαβαθμισμένο περιβάλλον ΤΠΕ της οικείας οντότητας της Ένωσης, συμπεριλαμβανομένων τυχόν περιβάλλοντος ΤΠΕ και δικτύου λειτουργικής τεχνολογίας εντός των εγκαταστάσεων, καθώς και 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 τα εν λόγω περιβάλλοντα («περιβάλλον ΤΠΕ»). Το πλαίσιο βασίζεται σε ολιστική προσέγγιση των κινδύνων.

3. Το πλαίσιο διασφαλίζει υψηλό επίπεδο κυβερνοασφάλειας. Το πλαίσιο καθορίζει εσωτερικές πολιτικές κυβερνοασφάλειας, συμπεριλαμβανομένων στόχων και προτεραιοτήτων, για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, καθώς και τους ρόλους και τις αρμοδιότητες του προσωπικού της οντότητας της Ένωσης που είναι επιφορτισμένο με τη διασφάλιση της αποτελεσματικής εφαρμογής του παρόντος κανονισμού. Το πλαίσιο περιλαμβάνει επίσης μηχανισμούς για τη μέτρηση της αποτελεσματικότητας της εφαρμογής.

4. Το πλαίσιο επανεξετάζεται τακτικά, υπό το πρίσμα των μεταβαλλόμενων κινδύνων κυβερνοασφάλειας, και τουλάχιστον ανά τετραετία. Κατά περίπτωση και κατόπιν αιτήματος του διοργανικού συμβουλίου κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10, το πλαίσιο οντότητας της Ένωσης μπορεί να επικαιροποιείται με βάση την καθοδήγηση της CERT-ΕΕ σχετικά με περιστατικά που καταγράφονται ή πιθανά κενά που παρατηρούνται κατά την εφαρμογή του παρόντος κανονισμού.

5. Το ανώτατο διοικητικό επίπεδο κάθε οντότητας της Ένωσης είναι υπεύθυνο για την εφαρμογή του παρόντος κανονισμού και επιβλέπει τη συμμόρφωση της οργάνωσής της με τις υποχρεώσεις που σχετίζονται με το πλαίσιο.

6. Κατά περίπτωση και με την επιφύλαξη της ευθύνης του για την εφαρμογή του παρόντος κανονισμού, το ανώτατο διοικητικό επίπεδο κάθε οντότητας της Ένωσης μπορεί να αναθέτει την εκπλήρωση συγκεκριμένων υποχρεώσεων δυνάμει του παρόντος κανονισμού σε ανώτερους υπαλλήλους κατά την έννοια του άρθρου 29 παράγραφος 2 του κανονισμού υπηρεσιακής κατάστασης ή σε άλλους υπαλλήλους ισοδύναμου επιπέδου, εντός της οικείας οντότητας της Ένωσης. Ανεξάρτητα από οποιαδήποτε τέτοια ανάθεση, το ανώτατο διοικητικό επίπεδο μπορεί να θεωρηθεί υπεύθυνο για παραβάσεις του παρόντος κανονισμού από την οικεία οντότητα της Ένωσης.

7. Κάθε οντότητα της Ένωσης εφαρμόζει αποτελεσματικούς μηχανισμούς για να διασφαλίζει ότι οι δαπάνες για την κυβερνοασφάλεια ανέρχονται σε επαρκές ποσοστό του προϋπολογισμού για την ΤΠΕ. Κατά τον καθορισμό του ποσοστού αυτού λαμβάνεται δεόντως υπόψη το πλαίσιο.

8. Κάθε οντότητα 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. Ο τοπικός υπεύθυνος κυβερνοασφάλειας διευκολύνει την εφαρμογή του παρόντος κανονισμού και υποβάλλει εκθέσεις απευθείας στο ανώτατο διοικητικό επίπεδο σε τακτική βάση σχετικά με την πορεία της εφαρμογής. Χωρίς να θίγεται ο ρόλος του τοπικού υπεύθυνου κυβερνοασφάλειας ως ενιαίου σημείου επαφής σε κάθε οντότητα της Ένωσης, μια οντότητα της Ένωσης μπορεί να αναθέτει στη CERT-ΕΕ ορισμένα καθήκοντα του τοπικού υπευθύνου κυβερνοασφάλειας όσον αφορά την εφαρμογή του παρόντος κανονισμού βάσει συμφωνίας σε επίπεδο υπηρεσιών που συνάπτεται μεταξύ της εν λόγω οντότητας της Ένωσης και της CERT-ΕΕ, ή τα εν λόγω καθήκοντα μπορούν να επιμερίζονται μεταξύ περισσότερων οντοτήτων της Ένωσης. Όταν τα καθήκοντα αυτά ανατίθενται στην CERT-ΕΕ, το διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10 αποφασίζει κατά πόσον η παροχή της υπηρεσίας αυτής αποτελεί μέρος των βασικών υπηρεσιών της CERT-ΕΕ, λαμβάνοντας υπόψη τους ανθρώπινους και οικονομικούς πόρους της οικείας οντότητας της Ένωσης. Κάθε οντότητα της Ένωσης ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση, τη CERT-ΕΕ σχετικά με τους διορισμένους τοπικούς υπεύθυνους κυβερνοασφάλειας και για κάθε μεταγενέστερη αλλαγή τους.

Η CERT-ΕΕ καταρτίζει και διατηρεί επίκαιρο κατάλογο των διορισμένων τοπικών υπευθύνων κυβερνοασφάλειας.

9. Οι ανώτεροι υπάλληλοι κατά την έννοια του άρθρου 29 παράγραφος 2 του κανονισμού υπηρεσιακής κατάστασης ή άλλοι υπάλληλοι ισοδύναμου επιπέδου κάθε οντότητας της Ένωσης, καθώς και όλα τα σχετικά μέλη του προσωπικού που είναι επιφορτισμένα με την εφαρμογή των μέτρων και την εκπλήρωση των υποχρεώσεων διαχείρισης κινδύνων κυβερνοασφάλειας του παρόντος κανονισμού, 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 της οντότητας της Ένωσης.

Άρθρο 7

Αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας

1. Έως τις … [18 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και στη συνέχεια τουλάχιστον ανά διετία, κάθε οντότητα της Ένωσης διενεργεί αξιολόγηση του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας που ενσωματώνει όλα τα στοιχεία του οικείου περιβάλλοντος ΤΠΕ.

2. Οι αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας διενεργούνται, κατά περίπτωση, με τη βοήθεια ειδικευμένου τρίτου μέρους.

3. Οι οντότητες της Ένωσης με παρόμοιες δομές μπορούν να συνεργάζονται για τη διενέργεια αξιολογήσεων του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας για τις αντίστοιχες οντότητές τους.

4. Βάσει αιτήματος του διοργανικού συμβουλίου κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10, και με τη ρητή συγκατάθεση της οικείας οντότητας της Ένωσης, τα αποτελέσματα αξιολόγησης του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας μπορούν να συζητούνται στο πλαίσιο του εν λόγου συμβουλίου ή της άτυπης ομάδας τοπικών υπευθύνων κυβερνοασφάλειας, με σκοπό την άντληση διδαγμάτων από την εμπειρία και την ανταλλαγή βέλτιστων πρακτικών.

Άρθρο 8

Μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας

1. Χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση έως τις … [20 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], κάθε οντότητα της Ένωσης, υπό την εποπτεία του ανώτατου διοικητικού επιπέδου της, λαμβάνει κατάλληλα και αναλογικά τεχνικά, λειτουργικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων κυβερνοασφάλειας που εντοπίζονται βάσει του πλαισίου, και για την πρόληψη ή την ελαχιστοποίηση του αντικτύπου των περιστατικών. Λαμβανομένης υπόψη της εξέλιξης της τεχνολογίας και, κατά περίπτωση, των σχετικών ευρωπαϊκών και διεθνών προτύπων, τα εν λόγω μέτρα διασφαλίζουν επίπεδο ασφάλειας των δικτυακών και πληροφοριακών συστημάτων σε ολόκληρο το περιβάλλον ΤΠΕ ανάλογο προς τους εμφανιζόμενους κινδύνους κυβερνοασφάλειας. Κατά την αξιολόγηση της αναλογικότητας των εν λόγω μέτρων, λαμβάνεται δεόντως υπόψη ο βαθμός έκθεσης της οντότητας της Ένωσης σε κινδύνους κυβερνοασφάλειας, το μέγεθός της, και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένου του κοινωνικού, οικονομικού και διοργανικού αντικτύπου τους.

2. Οι οντότητες της Ένωσης λαμβάνουν υπόψη τουλάχιστον τους ακόλουθους τομείς κατά την εφαρμογή των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας:

α) πολιτική κυβερνοασφάλειας, συμπεριλαμβανομένων των μέτρων που απαιτούνται για την επίτευξη των στόχων και των προτεραιοτήτων που αναφέρονται στο άρθρο 6 και στην παράγραφο 3 του παρόντος άρθρου·

β) πολιτικές για την ανάλυση κινδύνων κυβερνοασφάλειας και την ασφάλεια των πληροφοριακών συστημάτων·

γ) στόχους πολιτικής σχετικά με τη χρήση υπηρεσιών υπολογιστικού νέφους·

δ) έλεγχο κυβερνοασφάλειας, κατά περίπτωση, ο οποίος μπορεί να περιλαμβάνει αξιολόγηση κινδύνων κυβερνοασφάλειας, ευπαθειών και κυβερνοαπειλών, και δοκιμές διείσδυσης που διενεργούνται από αξιόπιστο ιδιωτικό πάροχο σε τακτική βάση·

ε) εφαρμογή των συστάσεων που προκύπτουν από τους ελέγχους κυβερνοασφάλειας που αναφέρονται στο στοιχείο δ) μέσω επικαιροποιήσεων για την κυβερνοασφάλεια και επικαιροποιήσεων πολιτικής·

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

ζ) διαχείριση περιουσιακών στοιχείων, συμπεριλαμβανομένης της απογραφής περιουσιακών στοιχείων ΤΠΕ και της χαρτογράφησης του δικτύου ΤΠΕ·

η) ασφάλεια ανθρώπινων πόρων και έλεγχο πρόσβαση·

θ) ασφάλεια των επιχειρήσεων·

ι) ασφάλεια των επικοινωνιών·

ια) απόκτηση, ανάπτυξη και συντήρηση συστημάτων, συμπεριλαμβανομένων πολιτικών για τον χειρισμό και τη γνωστοποίηση ευπαθειών·

ιβ) όπου είναι δυνατόν, πολιτικές για τη διαφάνεια του πηγαίου κώδικα·

ιγ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των πτυχών που αφορούν την ασφάλεια ως προς τις σχέσεις μεταξύ κάθε οντότητας της Ένωσης και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της·

ιδ) χειρισμός περιστατικών και συνεργασία με την CERT-EE, όπως η διατήρηση της παρακολούθησης και της καταγραφής ασφαλείας·

ιε) διαχείριση της επιχειρησιακής συνέχειας, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων· και

ιστ) προώθηση και ανάπτυξη προγραμμάτων εκπαίδευσης, απόκτησης δεξιοτήτων, ευαισθητοποίησης, πρακτικής εξάσκησης και κατάρτισης στον τομέα της κυβερνοασφάλειας.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο ιγ), οι οντότητες της Ένωσης λαμβάνουν υπόψη τις ιδιαίτερες ευπάθειες κάθε άμεσου προμηθευτή και παρόχου υπηρεσιών, καθώς και τη συνολική ποιότητα των προϊόντων και τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών τους, συμπεριλαμβανομένων των διαδικασιών ασφαλούς ανάπτυξής τους.

3. Οι οντότητες της Ένωσης λαμβάνουν τουλάχιστον τα ακόλουθα ειδικά μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας:

α) τεχνικές ρυθμίσεις για τη διευκόλυνση και τη διατήρηση της τηλεργασίας·

β) συγκεκριμένα μέτρα για τη μετάβαση προς τις αρχές της μηδενικής εμπιστοσύνης·

γ) χρήση, κατά κανόνα, της πολυπαραγοντικής επαλήθευσης ταυτότητας σε όλα τα δικτυακά και πληροφοριακά συστήματα·

δ) χρήση της κρυπτογραφίας και της κρυπτογράφησης, ιδίως της διατερματικής κρυπτογράφησης, καθώς και της ασφαλούς ψηφιακής υπογραφής·

ε) κατά περίπτωση, ασφαλείς επικοινωνίες φωνής, βίντεο και κειμένου, και ασφαλή συστήματα επικοινωνίας έκτακτης ανάγκης εντός της οντότητας της Ένωσης·

στ) προδραστικά μέτρα για τον εντοπισμό και την αφαίρεση κακόβουλου λογισμικού και κατασκοπευτικού λογισμικού·

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

η) κατάρτιση και έγκριση εκπαιδευτικών προγραμμάτων για την κυβερνοασφάλεια ανάλογα με τα προβλεπόμενα καθήκοντα και τις αναμενόμενες ικανότητες για το ανώτατο επίπεδο διοίκησης και τα μέλη προσωπικού της οντότητας της Ένωσης στα οποία ανατίθεται η διασφάλιση της αποτελεσματικής εφαρμογής του παρόντος κανονισμού·

θ) τακτική κατάρτιση των μελών του προσωπικού σε θέματα κυβερνοασφάλειας·

ι) κατά περίπτωση, συμμετοχή σε αναλύσεις κινδύνου διασυνδεσιμότητας μεταξύ των οντοτήτων της Ένωσης·

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

i) της άρσης των συμβατικών φραγμών που περιορίζουν την κοινοποίηση από τους παρόχους υπηρεσιών ΤΠΕ στην CERT-ΕΕ πληροφοριών σχετικά με περιστατικά, ευπάθειες και κυβερνοαπειλές·

ii) συμβατικών υποχρεώσεων υποβολής εκθέσεων για περιστατικά, ευπάθειες και κυβερνοαπειλές, καθώς και εφαρμογής κατάλληλων μηχανισμών αντιμετώπισης και παρακολούθησης περιστατικών.

Άρθρο 9

Σχέδια κυβερνοασφάλειας

1. Έπειτα από την ολοκλήρωση της αξιολόγησης του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας που διενεργείται σύμφωνα με το άρθρο 7 και λαμβάνοντας υπόψη τα περιουσιακά στοιχεία και τους κινδύνους κυβερνοασφάλειας που προσδιορίζονται στο πλαίσιο, καθώς και τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας που λαμβάνονται σύμφωνα με το άρθρο 8, το ανώτατο διοικητικό επίπεδο κάθε οντότητας της Ένωσης εγκρίνει σχέδιο κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση έως τις … [24 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού]. Το σχέδιο κυβερνοασφάλειας αποσκοπεί στην αύξηση της συνολικής κυβερνοασφάλειας της οντότητας της Ένωσης και, ως εκ τούτου, συμβάλλει στην ενίσχυση του υψηλού κοινού επιπέδου κυβερνοασφάλειας εντός των οντοτήτων της Ένωσης. Το σχέδιο κυβερνοασφάλειας περιλαμβάνει τουλάχιστον τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας που λαμβάνονται σύμφωνα με το άρθρο 8. Το σχέδιο κυβερνοασφάλειας αναθεωρείται ανά διετία ή συχνότερα όταν είναι αναγκαίο, μετά τις αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας που διενεργούνται σύμφωνα με το άρθρο 7 ή μετά από οποιαδήποτε ουσιαστική επανεξέταση του πλαισίου.

2. Το σχέδιο κυβερνοασφάλειας περιλαμβάνει το σχέδιο της οντότητας της Ένωσης για τη διαχείριση κρίσεων στον κυβερνοχώρο όσον αφορά σοβαρά περιστατικά.

3. Η οντότητα της Ένωσης υποβάλλει το ολοκληρωμένο σχέδιο κυβερνοασφάλειας στο διοργανικό συμβούλιο κυβερνοασφάλειας που συγκροτείται σύμφωνα με το άρθρο 10.

Κεφάλαιο III

Διοργανικό συμβούλιο κυβερνοασφάλειας

Άρθρο 10

Διοργανικό συμβούλιο κυβερνοασφάλειας

1. Ιδρύεται διοργανικό συμβούλιο κυβερνοασφάλειας («ΔΣΚ»).

2. Το ΔΣΚ είναι αρμόδιο για:

   α) την παρακολούθηση και την υποστήριξη της εφαρμογής του παρόντος κανονισμού από τις οντότητες της Ένωσης·

   β) την εποπτεία της υλοποίησης των γενικών προτεραιοτήτων και στόχων από την CERT-EE και την παροχή στρατηγικών κατευθύνσεων στην CERT-EE.

3. Το ΔΣΚ αποτελείται από:

   α) έναν εκπρόσωπο που ορίζει καθένας από τους ακόλουθους φορείς:

      i) το Ευρωπαϊκό Κοινοβούλιο·

      ii) το Ευρωπαϊκό Συμβούλιο·

iii) το Συμβούλιο της Ευρωπαϊκής Ένωσης·

iv) η Επιτροπή·

v) το Δικαστήριο της Ευρωπαϊκής Ένωσης·

vi) η Ευρωπαϊκή Κεντρική Τράπεζα·

vii) το Ελεγκτικό Συνέδριο·

viii) η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης·

ix) η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή·

x) η Ευρωπαϊκή Επιτροπή των Περιφερειών·

xi) η Ευρωπαϊκή Τράπεζα Επενδύσεων·

xii) το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας·

xiii) ο ENISA·

xiv) ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ)·

xv) ο Οργανισμός της Ευρωπαϊκής Ένωσης για το Διαστημικό Πρόγραμμα.

β) τρεις εκπροσώπους τους οποίους ορίζει το Δίκτυο Οργανισμών της ΕΕ («EUAN») βάσει πρότασης της συμβουλευτικής επιτροπής ΤΠΕ του εν λόγω Δικτύου για να εκπροσωπούν τα συμφέροντα των λοιπών οργάνων και οργανισμών της Ένωσης που διαχειρίζονται το δικό τους περιβάλλον ΤΠΕ, πέραν αυτών που αναφέρονται στο στοιχείο α).

Οι οντότητες της Ένωσης που εκπροσωπούνται στο ΔΣΚ επιδιώκουν την επίτευξη ισόρροπης εκπροσώπησης των φύλων μεταξύ των ορισθέντων εκπροσώπων.

4. Τα μέλη του ΔΣΚ μπορούν να επικουρούνται από αναπληρωτή. Ο πρόεδρος μπορεί να προσκαλεί και άλλους εκπροσώπους των οντοτήτων της Ένωσης που αναφέρονται στην παράγραφο 3 ή άλλων οντοτήτων της Ένωσης να παραστούν στις συνεδριάσεις του ΔΣΚ χωρίς δικαίωμα ψήφου.

5. Ο επικεφαλής της CERT-ΕΕ και οι πρόεδροι της Ομάδας Συνεργασίας, του δικτύου CSIRT και του EU-CyCLONe που συγκροτούνται σύμφωνα με τα άρθρα 14, 15 και 16, αντίστοιχα, της οδηγίας (ΕΕ) 2022/2555, ή οι αναπληρωτές τους, μπορούν να συμμετέχουν στις συνεδριάσεις του ΔΣΚ ως παρατηρητές. Σε εξαιρετικές περιπτώσειςΔΣΚ, το ΔΣΚ δύναται, σύμφωνα με τον εσωτερικό κανονισμό του, να αποφασίσει διαφορετικά.

6. Το ΔΣΚ θεσπίζει τον εσωτερικό κανονισμό του.

7. Το ΔΣΚ ορίζει πρόεδρο, σύμφωνα με τον εσωτερικό κανονισμό του, μεταξύ των μελών του για τριετή θητεία. Το πρόσωπο που αναπληρώνει τον πρόεδρο καθίσταται τακτικό μέλος του ΔΣΚ για την ίδια θητεία.

8. Το ΔΣΚ συνεδριάζει τουλάχιστον τρεις φορές ανά έτος με πρωτοβουλία του προέδρου του, κατόπιν αιτήματος της CERT-EE ή κατόπιν αιτήματος οποιουδήποτε από τα μέλη του.

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

10. Το ΔΣΚ δύναται να ενεργεί με απλουστευμένη γραπτή διαδικασία που κινείται σύμφωνα με τον εσωτερικό κανονισμό τουΔΣΚ. Σύμφωνα με τη διαδικασία αυτή, η σχετική απόφαση θεωρείται εγκριθείσα εντός της προθεσμίας που ορίζει ο πρόεδρος, εκτός εάν ένα μέλος διατυπώσει αντιρρήσεις.

11. Η Επιτροπή παρέχει γραμματειακή υποστήριξη στο ΔΣΚ και η γραμματεία είναι υπόλογη στον πρόεδρο του ΔΣΚ.

12. Οι εκπρόσωποι που ορίζονται από το EUAN διαβιβάζουν τις αποφάσεις του ΔΣΚ στα μέλη του EUAN. Κάθε μέλος του EUAN έχει το δικαίωμα να επιστήσει την προσοχή των εν λόγω εκπροσώπων ή του προέδρου του ΔΣΚ σε οποιοδήποτε ζήτημα θεωρεί ότι πρέπει να τεθεί υπόψη του ΔΣΚ.

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

14. Έως τις … [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και, στη συνέχεια, σε ετήσια βάση, το ΔΣΚ υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, στην οποία περιγράφεται λεπτομερώς η πρόοδος που έχει σημειωθεί όσον αφορά την εφαρμογή του παρόντος κανονισμού και προσδιορίζεται ιδίως ο βαθμός συνεργασίας της CERT-ΕΕ με τους ομολόγους της σε κάθε κράτος μέλος. Η έκθεση παρέχει στοιχεία για την ανά διετία έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση που εγκρίνεται σύμφωνα με το άρθρο 18 της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 11

Καθήκοντα του ΔΣΚ

Κατά την άσκηση των αρμοδιοτήτων του, το ΔΣΚ ειδικότερα:

α) παρέχει καθοδήγηση στον επικεφαλής της CERT-ΕΕ·

β) παρακολουθεί και εποπτεύει αποτελεσματικά την εφαρμογή του παρόντος κανονισμού και στηρίζει τις οντότητες της Ένωσης στην ενίσχυση της κυβερνοασφάλειάς τους, μεταξύ άλλων ζητώντας, κατά περίπτωση, ad hoc εκθέσεις από τις οντότητες της Ένωσης και την CERT-ΕΕ·

γ) κατόπιν στρατηγικής συζήτησης, εγκρίνει πολυετή στρατηγική για την ενίσχυση του επιπέδου κυβερνοασφάλειας στις οντότητες της Ένωσης, αξιολογεί την εν λόγω στρατηγική σε τακτική βάση και τουλάχιστον ανά πενταετία και, κατά περίπτωση, τροποποιεί την εν λόγω στρατηγική·

δ) καθορίζει τη μεθοδολογία και τις οργανωτικές πτυχές για τη διενέργεια εθελοντικών αξιολογήσεων από ομοτίμους μεταξύ των οντοτήτων της Ένωσης, με σκοπό την άντληση διδαγμάτων από κοινές εμπειρίες, την ενίσχυση της αμοιβαίας εμπιστοσύνης, την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας, καθώς και την ενίσχυση των ικανοτήτων κυβερνοασφάλειας των οντοτήτων της Ένωσης, διασφαλίζοντας ότι οι εν λόγω αξιολογήσεις από ομοτίμους διενεργούνται από εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας που ορίζονται από οντότητα της Ένωσης διαφορετική από την αξιολογούμενη οντότητα της Ένωσης και ότι η μεθοδολογία βασίζεται στο άρθρο 19 της οδηγίας (ΕΕ) 2022/2555 και, κατά περίπτωση, προσαρμόζεται στις οντότητες της Ένωσης·

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

στ) εγκρίνει, βάσει πρότασης του επικεφαλής της CERT-ΕΕ, τον κατάλογο υπηρεσιών της CERT-ΕΕ και τυχόν επικαιροποιήσεις του·

ζ) εγκρίνει, βάσει πρότασης του επικεφαλής της CERT-ΕΕ, τον ετήσιο οικονομικό προγραμματισμό των εσόδων και των δαπανών, συμπεριλαμβανομένης της στελέχωσης, για τις δραστηριότητες της CERT-ΕΕ·

η) εγκρίνει, βάσει πρότασης του επικεφαλής της CERT-ΕΕ, τις ρυθμίσεις για τις συμφωνίες επιπέδου υπηρεσιών·

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

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

ια) εγκρίνει ρυθμίσεις συνεργασίας, συμφωνίες ή συμβάσεις σε επίπεδο υπηρεσιών μεταξύ της CERT-ΕΕ και άλλων οντοτήτων σύμφωνα με το άρθρο 18·

ιβ) εγκρίνει κατευθυντήριες γραμμές και συστάσεις βάσει πρότασης της CERT-ΕΕ σύμφωνα με το άρθρο 14 και αναθέτει στην CERT-ΕΕ να εκδώσει, να αποσύρει ή να τροποποιήσει πρόταση για κατευθυντήριες γραμμές ή συστάσεις, ή πρόσκληση για ανάληψη δράσης·

ιγ) συγκροτεί τεχνικές συμβουλευτικές ομάδες με συγκεκριμένα καθήκοντα, προκειμένου να συνδράμουν το ΔΣΚ στο έργο του, εγκρίνει την εντολή τους και ορίζει τον πρόεδρο κάθε ομάδας·

ιδ) λαμβάνει και αξιολογεί έγγραφα και εκθέσεις που υποβάλλουν οι οντότητες της Ένωσης δυνάμει του παρόντος κανονισμού, όπως αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας·

ιε) διευκολύνει τη σύσταση άτυπης ομάδας τοπικών υπευθύνων κυβερνοασφάλειας των οντοτήτων της Ένωσης, με την υποστήριξη του ENISA, με στόχο την ανταλλαγή βέλτιστων πρακτικών και πληροφοριών σε σχέση με την εφαρμογή του παρόντος κανονισμού·

ιστ) λαμβάνοντας υπόψη τις πληροφορίες που παρέχονται από την CERT-ΕΕ σχετικά με τους εντοπισθέντες κινδύνους κυβερνοασφάλειας και τα διδάγματα που αντλήθηκαν, παρακολουθεί την επάρκεια των ρυθμίσεων διασυνδεσιμότητας μεταξύ των περιβαλλόντων ΤΠΕ των οντοτήτων της Ένωσης και παρέχει συμβουλές σχετικά με πιθανές βελτιώσεις·

ιζ) καταρτίζει σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο με σκοπό τη στήριξη, σε επιχειρησιακό επίπεδο, της συντονισμένης διαχείρισης σοβαρών περιστατικών που επηρεάζουν οντότητες της Ένωσης, και τη συμβολή στην τακτική ανταλλαγή σχετικών πληροφοριών, ιδίως όσον αφορά τις επιπτώσεις και την κρισιμότητα σοβαρών περιστατικών και τους πιθανούς τρόπους μετριασμού των επιπτώσεών τους·

ιη) συντονίζει την έγκριση των σχεδίων διαχείρισης κρίσεων στον κυβερνοχώρο που καταρτίζουν οι επιμέρους οντότητες της Ένωσης και τα οποία αναφέρονται στο άρθρο 9 παράγραφος 2·

ιθ) εκδίδει συστάσεις σχετικά με την ασφάλεια στον κυβερνοχώρο που αναφέρονται στο άρθρο 8 παράγραφος 2 πρώτο εδάφιο στοιχείο ιγ), λαμβάνοντας υπόψη τα αποτελέσματα των συντονισμένων σε ενωσιακό επίπεδο εκτιμήσεων κινδύνου για τις κρίσιμες αλυσίδες εφοδιασμού που αναφέρονται στο άρθρο 22 της οδηγίας (ΕΕ) 2022/2555, για να στηρίξει τις οντότητες της Ένωσης στη θέσπιση αποτελεσματικών και αναλογικών μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας.

Άρθρο 12

Συμμόρφωση

1. Το ΔΣΚ, σύμφωνα με το άρθρο 10 παράγραφος 2 και το άρθρο 11, παρακολουθεί αποτελεσματικά την εφαρμογή του παρόντος κανονισμού και των εκδοθεισών κατευθυντήριων γραμμών, συστάσεων και εκκλήσεων για ανάληψη δράσης από τις οντότητες της Ένωσης. Το ΔΣΚ μπορεί να ζητεί από τις οντότητες της Ένωσης πληροφορίες ή έγγραφα που απαιτούνται για τον σκοπό αυτό. Για τους σκοπούς της έγκρισης μέτρων συμμόρφωσης δυνάμει του παρόντος άρθρου, όταν η οικεία οντότητα της Ένωσης εκπροσωπείται άμεσα στο ΔΣΚ, δεν έχει δικαίωμα ψήφου.

2. Όταν το ΔΣΚ διαπιστώνει ότι μια οντότητα της Ένωσης δεν έχει εφαρμόσει αποτελεσματικά τον παρόντα κανονισμό ή τις κατευθυντήριες γραμμές, τις συστάσεις ή τις εκκλήσεις για ανάληψη δράσης που εκδίδονται δυνάμει αυτού, δύναται, με την επιφύλαξη των εσωτερικών διαδικασιών της οικείας οντότητας της Ένωσης, και αφού δώσει στην οικεία οντότητα της Ένωσης την ευκαιρία να παρουσιάσει τις παρατηρήσεις της:

   α) να κοινοποιήσει αιτιολογημένη γνώμη στην οντότητα της Ένωσης σχετικά με παρατηρηθέντα κενά στην εφαρμογή του παρόντος κανονισμού·

   β) να παράσχει, κατόπιν διαβούλευσης με την CERT-ΕΕ, κατευθυντήριες γραμμές στην οικεία οντότητα της Ένωσης προκειμένου να διασφαλίσει ότι το πλαίσιό της, τα μέτρα της για τη διαχείριση κινδύνων κυβερνοασφάλειας, το σχέδιο κυβερνοασφάλειάς της και οι εκθέσεις της συμμορφώνονται με τον παρόντα κανονισμό εντός καθορισμένης περιόδου·

γ) να εκδώσει προειδοποίηση για την αντιμετώπιση, εντός καθορισμένης προθεσμίας, ελλείψεων που εντοπίστηκαν, συμπεριλαμβανομένων συστάσεων για την τροποποίηση μέτρων που εγκρίθηκαν από την οικεία οντότητα της Ένωσης σύμφωνα με τον παρόντα κανονισμό·

δ) να εκδώσει αιτιολογημένη κοινοποίηση προς την οικεία οντότητα της Ένωσης, σε περίπτωση που οι εντοπισθείσες ελλείψεις που προσδιορίζονται σε προειδοποίηση που εκδόθηκε σύμφωνα με το στοιχείο γ) δεν αντιμετωπίστηκαν επαρκώς εντός της καθορισμένης προθεσμίας·

ε) να εκδώσει:

i) σύσταση για τη διενέργεια ελέγχου· ή

ii) αίτημα διενέργειας ελέγχου από τρίτο φορέα παροχής υπηρεσιών ελέγχου·

στ) κατά περίπτωση, να ενημερώσει το Ελεγκτικό Συνέδριο, στο πλαίσιο της εντολής του, για την εικαζόμενη μη συμμόρφωση·

ζ) να εκδώσει σύσταση ώστε όλα τα κράτη μέλη και όλες οι οντότητες της Ένωσης να εφαρμόσουν προσωρινή αναστολή των ροών δεδομένων προς την οικεία οντότητα της Ένωσης.

Για τους σκοπούς του πρώτου εδαφίου στοιχείο γ), οι αποδέκτες μιας προειδοποίησης περιορίζονται κατάλληλα, όταν αυτό είναι αναγκαίο λόγω του κινδύνου κυβερνοασφάλειας.

Οι προειδοποιήσεις και οι συστάσεις που εκδίδονται σύμφωνα με το πρώτο εδάφιο απευθύνονται στο ανώτατο διοικητικό επίπεδο της οικείας οντότητας της Ένωσης.

3. Στις περιπτώσεις που το ΔΣΚ έχει εγκρίνει μέτρα σύμφωνα με την παράγραφο 2 πρώτο εδάφιο στοιχεία α) έως ζ), η οικεία οντότητα της Ένωσης παρέχει λεπτομερή στοιχεία σχετικά με τα μέτρα και τις δράσεις που έχουν αναληφθεί για την αντιμετώπιση των εικαζόμενων ελλείψεων που εντόπισε το ΔΣΚICB. Η οντότητα της Ένωσης υποβάλλει τα λεπτομερή αυτά στοιχεία εντός εύλογου χρονικού διαστήματος που συμφωνείται με το ΔΣΚ.

4. Όταν το ΔΣΚ θεωρεί ότι υπάρχει διαρκής παράβαση του παρόντος κανονισμού από οντότητα της Ένωσης ως άμεση απόρροια ενεργειών ή παραλείψεων υπαλλήλου ή μέλους της λοιπού προσωπικού της Ένωσης, συμπεριλαμβανομένων προσώπων στο ανώτατο διοικητικό επίπεδο, το ΔΣΚ ζητεί από την οικεία οντότητα της Ένωσης να λάβει τα κατάλληλα μέτρα, μεταξύ άλλων ζητώντας από την εν λόγω οντότητα να εξετάσει το ενδεχόμενο λήψης μέτρων πειθαρχικού χαρακτήρα σύμφωνα με τους κανόνες και τις διαδικασίες που ορίζονται στον κανονισμό υπηρεσιακής κατάστασης και οποιουσδήποτε άλλους εφαρμοστέους κανόνες και διαδικασίες. Για τον σκοπό αυτό, το ΔΣΚ διαβιβάζει τις απαραίτητες πληροφορίες στην οικεία οντότητα της Ένωσης.

5. Όταν οντότητες της Ένωσης κοινοποιούν ότι δεν είναι σε θέση να τηρήσουν τις προθεσμίες που ορίζονται στο άρθρο 6 παράγραφος 1 και στο άρθρο 8 παράγραφος 1, το ΔΣΚ μπορεί, σε δεόντως αιτιολογημένες περιπτώσεις και λαμβάνοντας υπόψη το μέγεθος της οντότητας της Ένωσης, να εγκρίνει την παράταση των εν λόγω προθεσμιών.

Κεφάλαιο IV
CERT-ΕΕ

Άρθρο 13

Αποστολή και καθήκοντα της CERT-ΕΕ

1. Αποστολή της CERT-ΕΕ είναι να συμβάλλει στην ασφάλεια του μη διαβαθμισμένου περιβάλλοντος ΤΠΕ των οντοτήτων της Ένωσης παρέχοντας σε αυτές συμβουλές σχετικά με την κυβερνοασφάλεια, συμβάλλοντας στην πρόληψη, στον εντοπισμό, στον χειρισμό, στον μετριασμό και στην αντιμετώπιση περιστατικών, καθώς και στην ανάκαμψη από περιστατικά, και λειτουργώντας για αυτές ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας.

2. Η CERT-ΕΕ συγκεντρώνει, διαχειρίζεται, αναλύει και ανταλλάσσει πληροφορίες με τις οντότητες της Ένωσης σχετικά με κυβερνοαπειλές, ευπάθειες και περιστατικά σε μη διαβαθμισμένες υποδομές ΤΠΕ. Συντονίζει την αντιμετώπιση περιστατικών σε διοργανικό επίπεδο και σε επίπεδο οντοτήτων της Ένωσης, μεταξύ άλλων παρέχοντας εξειδικευμένη επιχειρησιακή βοήθεια ή συντονίζοντας την παροχή της.

3. Η CERT-ΕΕ εκτελεί τα ακόλουθα καθήκοντα για να συνδράμει τις οντότητες της Ένωσης:

   α) τις στηρίζει κατά την εφαρμογή του παρόντος κανονισμού και συμβάλλει στον συντονισμό της εφαρμογής του παρόντος κανονισμού μέσω των μέτρων που παρατίθενται στο άρθρο 14 παράγραφος 1 ή μέσω ad-hoc εκθέσεων τις οποίες ζητά το ΔΣΚ·

β) προσφέρει τυπικές υπηρεσίες CSIRT για τις οντότητες της Ένωσης μέσω δέσμης υπηρεσιών κυβερνοασφάλειας που περιγράφονται στον κατάλογο υπηρεσιών της («βασικές υπηρεσίες»)·

γ) διατηρεί δίκτυο ομοτίμων και εταίρων για τη στήριξη των υπηρεσιών που περιγράφονται στα άρθρα 17 και 18·

δ) εφιστά την προσοχή του ΔΣΚ σε κάθε πρόβλημα που αφορά την εφαρμογή του παρόντος κανονισμού και την εφαρμογή των κατευθυντήριων γραμμών, των συστάσεων και των εκκλήσεων για ανάληψη δράσης·

ε) με βάση τις πληροφορίες που αναφέρονται στην παράγραφο 2, συμβάλλει στην επίγνωση της κατάστασης στον κυβερνοχώρο στην Ένωσης σε στενή συνεργασία με τον ENISA·

στ) συντονίζει τη διαχείριση σοβαρών περιστατικών·

ζ) ενεργεί εκ μέρους των οντοτήτων της Ένωσης ως το αντίστοιχο όργανο του συντονιστή που ορίζεται για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών σύμφωνα με το άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555·

η) παρέχει, κατόπιν αιτήματος οντότητας της Ένωσης, προδραστική μη παρεμβατική σάρωση δημόσια προσβάσιμων δικτυακών και πληροφοριακών συστημάτων της εν λόγω οντότητας της Ένωσης.

Οι πληροφορίες που αναφέρονται στο πρώτο εδάφιο στοιχείο ε) κοινοποιούνται στο ΔΣΚ, στο δίκτυο CSIRT και στο Κέντρο Ανάλυσης Πληροφοριών της Ευρωπαϊκής Ένωσης (EU INTCEN), κατά περίπτωση και όπου κρίνεται σκόπιμο, και με την επιφύλαξη των κατάλληλων όρων εμπιστευτικότητας.

4. Η CERT-ΕΕ μπορεί, σύμφωνα με το άρθρο 17 ή 18, κατά περίπτωση, να συνεργάζεται με σχετικές κοινότητες κυβερνοασφάλειας εντός της Ένωσης και των κρατών μελών της, μεταξύ άλλων στους ακόλουθους τομείς:

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

β) επιχειρησιακή συνεργασία όσον αφορά το δίκτυο CSIRT, μεταξύ άλλων όσον αφορά την αμοιβαία συνδρομή ·

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.

5. Στο πλαίσιο των αρμοδιοτήτων της, η CERT-ΕΕ συμμετέχει σε διαρθρωμένη συνεργασία με τον ENISA όσον αφορά την ανάπτυξη ικανοτήτων, την επιχειρησιακή συνεργασία και τις μακροπρόθεσμες στρατηγικές αναλύσεις των κυβερνοαπειλών σύμφωνα με τον κανονισμό (ΕΕ) 2019/881. Η CERT-ΕΕ μπορεί να συνεργάζεται και να ανταλλάσσει πληροφορίες με το Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα της Ευρωπόλ.

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

α) υπηρεσίες που υποστηρίζουν την κυβερνοασφάλεια του περιβάλλοντος ΤΠΕ των οντοτήτων της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 3, βάσει συμφωνιών επιπέδου υπηρεσιών και υπό την προϋπόθεση ότι υπάρχουν οι διαθέσιμοι πόροι, και συγκεκριμένα παρακολούθηση δικτύου ευρέος φάσματος, συμπεριλαμβανομένης της παρακολούθησης πρώτης γραμμής 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα για κυβερνοαπειλές υψηλής σοβαρότητας·

β) υπηρεσίες που υποστηρίζουν δραστηριότητες ή έργα των οντοτήτων της Ένωσης στον τομέα της κυβερνοασφάλειας, πέραν αυτών που αποσκοπούν στην προστασία του περιβάλλοντος ΤΠΕ των οντοτήτων αυτών, βάσει γραπτών συμφωνιών και με την προηγούμενη έγκριση του ΔΣΚ·

γ) κατόπιν αιτήματος, προδραστική σάρωση των δικτυακών και πληροφοριακών συστημάτων της οικείας οντότητας της Ένωσης για τον εντοπισμό ευπαθειών με δυνητικό σημαντικό αντίκτυπο·

δ) υπηρεσίες που υποστηρίζουν την ασφάλεια του περιβάλλοντος ΤΠΕ σε οργανισμούς άλλους πέραν των οντοτήτων της Ένωσης που συνεργάζονται στενά με οντότητες της Ένωσης, για παράδειγμα με την ανάθεση καθηκόντων ή αρμοδιοτήτων δυνάμει του ενωσιακού δικαίου, βάσει γραπτών συμφωνιών και με την προηγουμένη έγκριση του ΔΣΚ.

Όσον αφορά το πρώτο εδάφιο στοιχείο δ), η CERT-ΕΕ μπορεί, κατ' εξαίρεση, να συνάπτει συμφωνίες επιπέδου υπηρεσιών με άλλες οντότητες πέραν των οντοτήτων της Ένωσης, με προηγούμενη έγκριση του ΔΣΚ.

7. Η CERT-ΕΕ διοργανώνει και μπορεί να συμμετέχει σε ασκήσεις κυβερνοασφάλειας ή να συνιστά τη συμμετοχή σε υφιστάμενες ασκήσεις, κατά περίπτωση σε στενή συνεργασία με τον ENISA, με σκοπό τη δοκιμή του επιπέδου κυβερνοασφάλειας των οντοτήτων της Ένωσης.

8. Η CERT-ΕΕ μπορεί να παρέχει συνδρομή σε οντότητες της Ένωσης όσον αφορά περιστατικά σε δικτυακά και πληροφοριακά συστήματα που χειρίζονται ΔΠΕΕ, όταν αυτό ζητείται ρητά από τις οικείες οντότητες της Ένωσης σύμφωνα με τις αντίστοιχες διαδικασίες τους. Η παροχή συνδρομής από την CERT-ΕΕ δυνάμει της παρούσας παραγράφου δεν θίγει τους ισχύοντες κανόνες σχετικά με την προστασία διαβαθμισμένων πληροφοριών.

9. Η CERT-ΕΕ ενημερώνει τις οντότητες της Ένωσης σχετικά με τις διαδικασίες και διεργασίες που ακολουθεί για τον χειρισμό περιστατικών.

10. Η CERT-ΕΕ παρέχει, με υψηλό επίπεδο εμπιστευτικότητας και αξιοπιστίας, μέσω των κατάλληλων μηχανισμών συνεργασίας και διαύλων αναφοράς, σχετικές και ανωνυμοποιημένες πληροφορίες όσον αφορά σοβαρά περιστατικά και τον τρόπο με τον οποίο αντιμετωπίστηκαν. Οι πληροφορίες αυτές περιλαμβάνονται στην έκθεση που αναφέρεται στο άρθρο 10 παράγραφος 14.

11. Η CERT-ΕΕ, σε συνεργασία με τον ΕΕΠΔ, υποστηρίζει τις οικείες οντότητες της Ένωσης στην αντιμετώπιση περιστατικών που οδηγούν σε παραβιάσεις δεδομένων προσωπικού χαρακτήρα, με την επιφύλαξη της αρμοδιότητας και των καθηκόντων του ΕΕΠΔ ως εποπτικής αρχής δυνάμει του κανονισμού (ΕΕ) 2018/1725.

12. Η CERT-ΕΕ μπορεί, εφόσον ζητηθεί ρητά από τμήματα πολιτικής των οντοτήτων της Ένωσης, να συνεισφέρει τεχνικές συμβουλές ή στοιχεία για συναφή ζητήματα πολιτικής.

Άρθρο 14

Κατευθυντήριες γραμμές, 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 οι οντότητες της Ένωσης εντός καθορισμένου χρονικού πλαισίου·

β) προτάσεις προς το ΔΣΚ για κατευθυντήριες γραμμές που απευθύνονται σε όλες τις οντότητες της Ένωσης ή σε υποσύνολό τους·

γ) προτάσεις προς το ΔΣΚ για συστάσεις που απευθύνονται σε μεμονωμένες οντότητες της Ένωσης.

Όσον αφορά το πρώτο εδάφιο στοιχείο α), η οικεία οντότητα της Ένωσης ενημερώνει την CERT-ΕΕ, χωρίς αδικαιολόγητη καθυστέρηση μετά την παραλαβή της έκκλησης για ανάληψη δράσης, σχετικά με τον τρόπο με τον οποίο εφαρμόστηκαν τα επείγοντα μέτρα ασφάλειας.

2. Οι κατευθυντήριες γραμμές και οι συστάσεις μπορούν να περιλαμβάνουν:

α) κοινές μεθοδολογίες και ένα μοντέλο για την αξιολόγηση του επιπέδου ωριμότητας των οντοτήτων της Ένωσης στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των αντίστοιχων κλιμάκων ή ΒΔΕ, που χρησιμεύουν ως σημείο αναφοράς για τη στήριξη της συνεχούς βελτίωσης της κυβερνοασφάλειας σε όλες τις οντότητες της Ένωσης και διευκολύνουν την ιεράρχηση των τομέων και των μέτρων κυβερνοασφάλειας λαμβανομένης υπόψη της στάσης των οντοτήτων στον τομέα της κυβερνοασφάλειας·

β) ρυθμίσεις ή βελτιώσεις για τη διαχείριση κινδύνων κυβερνοασφάλειας και τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας·

γ) ρυθμίσεις για τις αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας και τα σχέδια κυβερνοασφάλειας·

δ) κατά περίπτωση, τη χρήση κοινής τεχνολογίας, κοινής αρχιτεκτονικής, ανοικτού κώδικα και κοινών συναφών βέλτιστων πρακτικών με στόχο την επίτευξη διαλειτουργικότητας και κοινών προτύπων, συμπεριλαμβανομένης μιας συντονισμένης προσέγγισης της ασφάλειας της εφοδιαστικής αλυσίδας·

ε) κατά περίπτωση, πληροφορίες για τη διευκόλυνση της χρήσης μέσων κοινών προμηθειών για την αγορά σχετικών υπηρεσιών και προϊόντων κυβερνοασφάλειας από τρίτους προμηθευτές·

στ) ρυθμίσεις ανταλλαγής πληροφοριών σύμφωνα με το άρθρο 20.

Άρθρο 15

Επικεφαλής της CERT-ΕΕ

1. Η Επιτροπή, αφού λάβει την έγκριση πλειοψηφίας δύο τρίτων των μελών του ΔΣΚ, διορίζει τον επικεφαλής της CERT-ΕΕ. Ζητείται η γνώμη του ΔΣΚ σε όλα τα στάδια της διαδικασίας διορισμού, ιδίως όσον αφορά τη σύνταξη προκηρύξεων κενής θέσης, την εξέταση των αιτήσεων και τον ορισμό των εξεταστικών επιτροπών σε σχέση με την εκάστοτε θέση. Η διαδικασία επιλογής, συμπεριλαμβανομένου του τελικού καταλόγου επικρατέστερων υποψηφίων μεταξύ των οποίων θα επιλεγεί το άτομο που θα διοριστεί στη θέση του επικεφαλής της CERT-ΕΕ, διασφαλίζει τη δίκαιη εκπροσώπηση κάθε φύλου, λαμβανομένων υπόψη των αιτήσεων που έχουν υποβληθεί.

2. Ο επικεφαλής της CERT-ΕΕ είναι αρμόδιος για την εύρυθμη λειτουργία της CERT-ΕΕ και ενεργεί στο πλαίσιο των αρμοδιοτήτων του ρόλου του υπό την καθοδήγηση του ΔΣΚ. Ο επικεφαλής της CERT-ΕΕ υποβάλλει τακτικά εκθέσεις στον πρόεδρο του ΔΣΚ και υποβάλλει ad hoc εκθέσεις στο ΔΣΚ κατόπιν αιτήματός του.

3. Ο επικεφαλής της CERT-ΕΕ συνδράμει τον αρμόδιο κύριο διατάκτη κατά τη σύνταξη της ετήσιας έκθεσης δραστηριοτήτων η οποία περιλαμβάνει δημοσιονομικές και διαχειριστικές πληροφορίες, μεταξύ των οποίων τα αποτελέσματα ελέγχων, και η οποία συντάσσεται βάσει του άρθρου 74 παράγραφος 9 του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1], και υποβάλλει τακτικά εκθέσεις στον κύριο διατάκτη σχετικά με την εφαρμογή των μέτρων για τα οποία έχει ανατεθεί αρμοδιότητα στον επικεφαλής της CERT-ΕΕ.

4. Ο επικεφαλής της CERT-ΕΕ καταρτίζει, σε ετήσια βάση, οικονομικό προγραμματισμό των διοικητικών εσόδων και δαπανών για τις δραστηριότητές της, το προτεινόμενο ετήσιο πρόγραμμα εργασίας, τον προτεινόμενο κατάλογο υπηρεσιών για την CERT-ΕΕ, προτεινόμενες αναθεωρήσεις του καταλόγου υπηρεσιών, προτεινόμενες ρυθμίσεις για συμφωνίες σε επίπεδο υπηρεσιών και προτεινόμενους ΒΔΕ για τη CERT-ΕΕ, που πρέπει να εγκριθούν από το ΔΣΚ σύμφωνα με το άρθρο 11. Κατά την αναθεώρηση του καταλόγου υπηρεσιών της CERT-ΕΕ, ο επικεφαλής της CERT-ΕΕ λαμβάνει υπόψη τους πόρους που διατίθενται στη CERT-ΕΕ.

---

[1] Κανονισμός (EU, 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).

5. Ο επικεφαλής της CERT-ΕΕ υποβάλλει εκθέσεις, τουλάχιστον σε ετήσια βάση, στο ΔΣΚ και στον πρόεδρο του ΔΣΚ σχετικά με τις δραστηριότητες και τις επιδόσεις της CERT-ΕΕ κατά την περίοδο αναφοράς, μεταξύ άλλων όσον αφορά 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 11. Οι εν λόγω εκθέσεις περιλαμβάνουν το πρόγραμμα εργασίας για την επόμενη περίοδο, τον δημοσιονομικό προγραμματισμό των εσόδων και των δαπανών, συμπεριλαμβανομένης της στελέχωσης, τις προγραμματισμένες επικαιροποιήσεις του καταλόγου υπηρεσιών της CERT-ΕΕ και αξιολόγηση του αναμενόμενου αντικτύπου που ενδέχεται να έχουν οι εν λόγω επικαιροποιήσεις όσον αφορά τους οικονομικούς και ανθρώπινους πόρους.

Άρθρο 16

Οικονομικά θέματα και θέματα προσωπικού

1. Η CERT-ΕΕ ενσωματώνεται στη διοικητική δομή μιας γενικής διεύθυνσης της Επιτροπής προκειμένου να επωφελείται από τις δομές υποστήριξης της Επιτροπής σε επίπεδο διοίκησης, δημοσιονομικής διαχείρισης και λογιστικής, διατηρώντας παράλληλα το καθεστώς της ως αυτόνομου διοργανικού παρόχου υπηρεσιών για όλες τις οντότητες της Ένωσης. Η Επιτροπή ενημερώνει το ΔΣΚ σχετικά με την διοικητική έδρα της CERT-EU καθώς και τυχόν αλλαγές της. Η Επιτροπή επανεξετάζει τις διοικητικές ρυθμίσεις που σχετίζονται με την CERT-ΕΕ σε τακτική βάση και σε κάθε περίπτωση πριν από τη θέσπιση οποιουδήποτε πολυετούς δημοσιονομικού πλαισίου σύμφωνα με το άρθρο 312 ΣΛΕΕ, ώστε να είναι δυνατή η λήψη κατάλληλων μέτρων. Η επανεξέταση περιλαμβάνει τη δυνατότητα σύστασης της CERT-ΕΕ ως γραφείου της Ένωσης.

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

3. Τα καθήκοντα και οι δραστηριότητες της CERT-ΕΕ, συμπεριλαμβανομένων των υπηρεσιών που παρέχονται από την CERT-ΕΕ σύμφωνα με το άρθρο 13 παράγραφοι 3, 4, 5, και 7 και το άρθρο 14 παράγραφος 1 στις οντότητες 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 θέσεις που προορίζονται για την CERT-ΕΕ περιγράφονται λεπτομερώς σε υποσημείωση του πίνακα προσωπικού της Επιτροπής.

4. Οι οντότητες της Ένωσης, πέραν αυτών που αναφέρονται στην παράγραφο 3 του παρόντος άρθρου, καταβάλλουν ετήσια χρηματοδοτική συνεισφορά στην CERT-ΕΕ για την κάλυψη των υπηρεσιών που παρέχει η CERT-ΕΕ σύμφωνα με την εν λόγω παράγραφο. Οι συνεισφορές βασίζονται σε κατευθύνσεις που παρέχει το ΔΣΚ και συμφωνούνται μεταξύ της κάθε οντότητας της Ένωσης 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 του παρόντος άρθρου, ως εσωτερικά έσοδα για ειδικό προορισμό, όπως προβλέπεται στο άρθρο 21 παράγραφος 3 στοιχείο γ) του κανονισμού (ΕΕ, Ευρατόμ) 2018/1046.

5. Οι δαπάνες για τις υπηρεσίες που προβλέπονται στο άρθρο 13 παράγραφος 6 ανακτώνται από τις οντότητες της Ένωσης που λαμβάνουν τις υπηρεσίες της CERT-ΕΕ. Τα έσοδα εγγράφονται στις γραμμές του προϋπολογισμού που καλύπτουν τις δαπάνες.

Άρθρο 17

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

1. Η CERT-ΕΕ συνεργάζεται και ανταλλάσσει πληροφορίες, χωρίς αδικαιολόγητη καθυστέρηση, με ομολόγους από κράτη μέλη, ιδίως τις CSIRT που ορίζονται ή συγκροτούνται σύμφωνα με το άρθρο 10 της οδηγίας (ΕΕ) 2022/2555 ή, κατά περίπτωση, τις αρμόδιες αρχές και τα ενιαία σημεία επαφής που ορίζονται ή συγκροτούνται σύμφωνα με το άρθρο 8 της εν λόγω οδηγίας, σχετικά με περιστατικά, κυβερνοαπειλές, ευπάθειες, παρ' ολίγον περιστατικά, πιθανά αντίμετρα, καθώς και βέλτιστες πρακτικές και όλα τα θέματα που αφορούν τη βελτίωση της προστασίας των περιβαλλόντων ΤΠΕ των οντοτήτων της Ένωσης, μεταξύ άλλων μέσω του δικτύου CSIRT που συγκροτείται σύμφωνα με το άρθρο 15 της οδηγίας (ΕΕ) 2022/2555. Η CERT-ΕΕ στηρίζει την Επιτροπή στο EU- CyCLONe που συγκροτείται σύμφωνα με το άρθρο 16 της οδηγίας (ΕΕ) 2022/2555 για τη συντονισμένη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

2. Όταν η CERT-EU αντιλαμβάνεται σημαντικό περιστατικό που λαμβάνει χώρα στην επικράτεια ενός κράτους μέλους, ενημερώνει, χωρίς καθυστέρηση, κάθε σχετικό ομόλογό της στο εν λόγω κράτος μέλος, σύμφωνα με την παράγραφο 1.

3. Υπό την προϋπόθεση ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται σύμφωνα με την ισχύουσα νομοθεσία της Ένωσης για την προστασία των δεδομένων, η CERT-ΕΕ ανταλλάσσει με ομολόγους της από κράτη μέλη, χωρίς αδικαιολόγητη καθυστέρηση, σχετικές πληροφορίες που αφορούν συγκεκριμένα περιστατικά οι οποίες διευκολύνουν τον εντοπισμό παρόμοιων κυβερνοαπειλών ή περιστατικών, ή συμβάλλουν στην ανάλυση περιστατικού, χωρίς την άδεια της θιγόμενης οντότητας της Ένωσης. Η CERT-ΕΕ ανταλλάσσει πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού μόνο όταν συντρέχει μία από τις ακόλουθες περιπτώσεις:

α) η θιγόμενη οντότητα της Ένωσης δίνει τη συγκατάθεσή της·

β) η θιγόμενη οντότητα της Ένωσης δεν δίνει τη συγκατάθεσή της όπως προβλέπεται στο στοιχείο α), αλλά η γνωστοποίηση της ταυτότητας της θιγόμενης οντότητας της Ένωσης θα αύξανε την πιθανότητα αποφυγής ή μετριασμού περιστατικών αλλού·

γ) η θιγόμενη οντότητα της Ένωσης έχει ήδη δημοσιοποιήσει ότι επηρεάστηκε.

Οι αποφάσεις για την ανταλλαγή πληροφοριών σχετικά με συγκεκριμένα περιστατικά οι οποίες αποκαλύπτουν την ταυτότητα του στόχου του περιστατικού σύμφωνα με το πρώτο εδάφιο στοιχείο β), εγκρίνονται από τον επικεφαλής της CERT-ΕΕ. Πριν από την έκδοση της εν λόγω απόφασης, η CERT-ΕΕ επικοινωνεί γραπτώς με τη θιγόμενη οντότητα της Ένωσης, εξηγώντας με σαφήνεια τον τρόπο με τον οποίο η γνωστοποίησή της ταυτότητάς της θα συνέβαλε στην αποφυγή ή τον μετριασμό περιστατικών αλλού. Ο επικεφαλής της CERT-ΕΕ παρέχει τις εξηγήσεις και ζητεί ρητά από την οντότητα της Ένωσης να δηλώσει εάν δίνει τη συγκατάθεσή της εντός καθορισμένης προθεσμίας. Ο επικεφαλής της CERT-ΕΕ ενημερώνει επίσης την οντότητα της Ένωσης ότι, υπό το πρίσμα των εξηγήσεων που παρέχονται, διατηρεί το δικαίωμα να γνωστοποιήσει τις πληροφορίες ακόμη και ελλείψει συγκατάθεσης. Η θιγόμενη οντότητα της Ένωσης ενημερώνεται πριν από τη γνωστοποίηση των πληροφοριών.

Άρθρο 18

Συνεργασία της CERT-ΕΕ με άλλους ομολόγους

1. Η CERT-ΕΕ μπορεί να συνεργάζεται με ομολόγους της στην Ένωση πέραν αυτών που αναφέρονται στο άρθρο 17 οι οποίοι υπόκεινται σε ενωσιακές απαιτήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων ομολόγων ανά κλάδο, σχετικά με εργαλεία και μεθόδους, όπως τεχνικές, τακτικές, διαδικασίες και βέλτιστες πρακτικές, καθώς και σχετικά με κυβερνοαπειλές και ευπάθειες. Για κάθε συνεργασία με τους εν λόγω ομολόγους, η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΔΣΚ κατά περίπτωση. Όταν η CERT-ΕΕ αναπτύσσει συνεργασία με ομολόγους αυτού του είδους, ενημερώνει τυχόν σχετικούς ομολόγους από τα κράτη μέλη οι οποίοι αναφέρονται στο άρθρο 17 παράγραφος 1, στο κράτος μέλος στο οποίο βρίσκεται ο ομόλογος. Κατά περίπτωση και όπου κρίνεται σκόπιμο, η εν λόγω συνεργασία και οι όροι της, μεταξύ άλλων όσον αφορά την κυβερνοασφάλεια, την προστασία των δεδομένων και τον χειρισμό πληροφοριών, θεσπίζονται με ειδικές ρυθμίσεις εμπιστευτικότητας, όπως συμβάσεις ή διοικητικές ρυθμίσεις. Για τις ρυθμίσεις εμπιστευτικότητας δεν απαιτείται εκ των προτέρων έγκριση από το ΔΣΚ, αλλά ο πρόεδρός του πρέπει να ενημερώνεται σχετικά. Σε περίπτωση επείγουσας και άμεσης ανάγκης ανταλλαγής πληροφοριών κυβερνοασφάλειας προς το συμφέρον οντοτήτων της Ένωσης ή άλλου μέρους, η CERT-ΕΕ μπορεί να προβεί σε τέτοια συνεργασία με οντότητα της οποίας η ειδική αρμοδιότητα, ικανότητα και εμπειρογνωσία απαιτούνται δικαιολογημένα για τη συνδρομή στην εν λόγω επείγουσα και άμεση ανάγκη, ακόμη και αν η CERT-ΕΕ δεν έχει συνάψει ρύθμιση εμπιστευτικότητας με την εν λόγω οντότητα. Στις περιπτώσεις αυτές, η CERT-ΕΕ ενημερώνει αμέσως τον πρόεδρο του ΔΣΚ και ενημερώνει το ΔΣΚ μέσω τακτικών εκθέσεων ή συνεδριάσεων.

2. Η CERT-ΕΕ μπορεί να συνεργάζεται με άλλους εταίρους, όπως εμπορικές οντότητες, συμπεριλαμβανομένων των βιομηχανικών οντοτήτων ανά τομέα, διεθνείς οργανισμούς, εθνικές οντότητες εκτός Ευρωπαϊκής Ένωσης ή μεμονωμένους εμπειρογνώμονες, για τη συλλογή πληροφοριών σχετικά με γενικές και ειδικές κυβερνοαπειλές, παρ' ολίγον περιστατικά, ευπάθειες και πιθανά αντίμετρα. Για ευρύτερη συνεργασία με τους εταίρους αυτούς, η CERT-ΕΕ ζητεί την προηγούμενη έγκριση του ΔΣΚ κατά περίπτωση.

3. Η CERT-ΕΕ μπορεί, με τη συγκατάθεση της οντότητας της Ένωσης που επηρεάζεται από περιστατικό και υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία ή σύμβαση τήρησης του απορρήτου με τον σχετικό ομόλογο ή εταίρο, να παρέχει πληροφορίες σχετικά με το συγκεκριμένο περιστατικό σε ομολόγους ή εταίρους που αναφέρονται στις παραγράφους 1 και 2 αποκλειστικά με σκοπό να συμβάλει στην ανάλυσή του.

Κεφάλαιο V

Υποχρεώσεις συνεργασίας και υποβολής αναφορών

Άρθρο 19

Χειρισμός πληροφοριών

1. Οι οντότητες της Ένωσης και η CERT-ΕΕ τηρούν την υποχρέωση τήρησης του επαγγελματικού απορρήτου σύμφωνα με το άρθρο 339 ΣΛΕΕ ή ισοδύναμα εφαρμοστέα πλαίσια.

2. Ο κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1] εφαρμόζεται 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 άλλες οντότητες της Ένωσης ή, κατά περίπτωση, με τα κράτη μέλη, όταν το αίτημα αφορά τα έγγραφά τους.

3. Ο χειρισμός πληροφοριών από τις οντότητες της Ένωσης και την CERT-ΕΕ συνάδει με τους ισχύοντες κανόνες για την ασφάλεια των πληροφοριών.

Άρθρο 20

Ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της κυβερνοασφάλειας

1. Οι οντότητες της Ένωσης μπορούν, σε εθελοντική βάση, να κοινοποιούν στην CERT-ΕΕ περιστατικά, κυβερνοαπειλές, παρ' ολίγον περιστατικά και ευπάθειες που τις επηρεάζουν, και να της παρέχουν σχετικές πληροφορίες. Η CERT-ΕΕ εξασφαλίζει ότι διατίθενται αποτελεσματικά μέσα επικοινωνίας, με υψηλό βαθμό ιχνηλασιμότητας, εμπιστευτικότητας και αξιοπιστίας, για τη διευκόλυνση της ανταλλαγής πληροφοριών με τις οντότητες της Ένωσης. Κατά την επεξεργασία κοινοποιήσεων, η CERT-ΕΕ μπορεί να δίνει προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων. Με την επιφύλαξη του άρθρου 12, η εθελούσια κοινοποίηση δεν συνεπάγεται την επιβολή στην αναφέρουσα οντότητα της Ένωσης πρόσθετων υποχρεώσεων τις οποίες δεν θα υπείχε αν δεν προέβαινε στην κοινοποίηση.

[1] 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).

2. Για να εκτελεί την αποστολή και τα καθήκοντα που της ανατίθενται σύμφωνα με το άρθρο 13, η CERT-ΕΕ μπορεί να ζητεί από τις οντότητες της Ένωσης να της παρέχουν πληροφορίες από τις αντίστοιχες απογραφές των οικείων συστημάτων ΤΠΕ, συμπεριλαμβανομένων πληροφοριών σχετικά με κυβερνοαπειλές, παρ' ολίγον περιστατικά, ευπάθειες, δείκτες έκθεσης σε κίνδυνο, ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό περιστατικών. Η οντότητα στην οποία υποβάλλεται το αίτημα διαβιβάζει τις ζητούμενες πληροφορίες, καθώς και τυχόν μεταγενέστερες επικαιροποιήσεις τους, χωρίς αδικαιολόγητη καθυστέρηση.

3. Η CERT-ΕΕ μπορεί να ανταλλάσσει με τις οντότητες της Ένωσης πληροφορίες σχετικά με συγκεκριμένα περιστατικά που αποκαλύπτουν την ταυτότητα της επηρεαζόμενης από το περιστατικό οντότητας της Ένωσης, εφόσον η εν λόγω οντότητα της Ένωσης δώσει τη συγκατάθεσή της. Όταν οντότητα της Ένωσης αρνείται να δώσει τη συγκατάθεσή της, παρέχει στην CERT-ΕΕ τους λόγους που τεκμηριώνουν την εν λόγω απόφαση.

4. Οι οντότητες της Ένωσης ανταλλάσσουν, κατόπιν αιτήματος, πληροφορίες με το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την ολοκλήρωση των σχεδίων κυβερνοασφάλειας.

5. Το ΔΣΚ ή η CERT-ΕΕ, κατά περίπτωση, κοινοποιεί, κατόπιν αιτήματος, κατευθυντήριες γραμμές, συστάσεις και εκκλήσεις για ανάληψη δράσης στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.

6. Οι υποχρεώσεις ανταλλαγής που ορίζονται στο παρόν άρθρο δεν επεκτείνονται σε:

α) ΔΠΕΕ·

β) πληροφορίες των οποίων η περαιτέρω διανομή έχει αποκλειστεί μέσω ορατής σήμανσης, εκτός εάν έχει επιτραπεί ρητά η κοινοποίησή τους στην CERT-ΕΕ.

Άρθρο 21

Υποχρεώσεις υποβολής εκθέσεων

1. Ένα περιστατικό θεωρείται σημαντικό εάν:

α) έχει προκαλέσει ή είναι σε θέση να προκαλέσει σοβαρή λειτουργική διατάραξη ή οικονομική ζημία στην οικεία οντότητα της Ένωσης·

β) έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

2. Οι οντότητες της Ένωσης υποβάλλουν στη CERT-ΕΕ:

α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, έγκαιρη προειδοποίηση, η οποία, κατά περίπτωση, αναφέρει αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από έκνομες ή κακόβουλες ενέργειες ή θα μπορούσε να έχει αντίκτυπο μεταξύ οντοτήτων ή διασυνοριακό αντίκτυπο·

β) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή που έγινε αντιληπτό το σημαντικό περιστατικό, κοινοποίηση περιστατικού, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες που αναφέρονται στο στοιχείο α) και αναφέρει μια αρχική αξιολόγηση του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και του αντικτύπου του, καθώς και, εφόσον υπάρχουν, τις ενδείξεις της προσβολής·

γ) κατόπιν αιτήματος της CERT-ΕΕ, ενδιάμεση έκθεση όσον αφορά τις σχετικές επικαιροποιήσεις της κατάστασης·

δ) τελική έκθεση το αργότερο ένα μήνα μετά την υποβολή της κοινοποίησης περιστατικού σύμφωνα με το στοιχείο β), η οποία περιλαμβάνει τα ακόλουθα:

i) λεπτομερή περιγραφή του περιστατικού, συμπεριλαμβανομένων της σοβαρότητάς του και του αντικτύπου του·

ii) το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό·

iii) τα εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού·

iv) κατά περίπτωση, τον διασυνοριακό αντίκτυπο του περιστατικού ή τον αντίκτυπό του μεταξύ οντοτήτων·

ε) σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης που αναφέρεται στο στοιχείο δ), έκθεση προόδου τη δεδομένη στιγμή και τελική έκθεση εντός ενός μηνός από τον εκ μέρους τους χειρισμό του περιστατικού.

3. Μια οντότητα της Ένωσης ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έγινε αντιληπτό σημαντικό περιστατικό, τυχόν σχετικούς ομολόγους από τα κράτη μέλη οι οποίοι αναφέρονται στο άρθρο 17 παράγραφος 1, στο κράτος μέλος στο οποίο βρίσκεται ο ομόλογος, ότι έχει συμβεί σημαντικό περιστατικό.

4. Οι οντότητες της Ένωσης αναφέρουν, μεταξύ άλλων, κάθε πληροφορία που επιτρέπει στην CERT-ΕΕ να προσδιορίσει τυχόν αντίκτυπο μεταξύ οντοτήτων, αντίκτυπο στο κράτος μέλος υποδοχής ή διασυνοριακό αντίκτυπο μετά από σημαντικό περιστατικό. Με την επιφύλαξη του άρθρου 12, η απλή πράξη κοινοποίησης δεν συνεπάγεται αυξημένη ευθύνη της οντότητας της Ένωσης.

5. Κατά περίπτωση, οι οντότητες της Ένωσης κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στους χρήστες των επηρεαζόμενων δικτυακών και πληροφοριακών συστημάτων ή άλλων συνιστωσών του περιβάλλοντος ΤΠΕ, που ενδέχεται να επηρεαστούν από σημαντικό περιστατικό ή σημαντική κυβερνοαπειλή, και, κατά περίπτωση, πρέπει να λάβουν μέτρα μετριασμού, τυχόν μέτρα ή διορθωτικές ενέργειες στις οποίες μπορούν να προβούν για την αντιμετώπιση του εν λόγω περιστατικού ή της εν λόγω απειλής. Κατά περίπτωση, οι οντότητες της Ένωσης ενημερώνουν τους εν λόγω χρήστες για την ίδια τη σημαντική κυβερνοαπειλή.

6. Όταν σημαντικό περιστατικό ή σημαντική κυβερνοαπειλή επηρεάζει δικτυακό ή πληροφοριακό σύστημα ή συνιστώσα περιβάλλοντος ΤΠΕ οντότητας της Ένωσης που είναι γνωστό ότι είναι συνδεδεμένη με το περιβάλλον ΤΠΕ άλλης οντότητας της Ένωσης, η CERT-ΕΕ εκδίδει σχετική ειδοποίηση επαγρύπνησης για την κυβερνοασφάλεια.

7. Οι οντότητες της Ένωσης, κατόπιν αιτήματος της CERT-ΕΕ και χωρίς αδικαιολόγητη καθυστέρηση, παρέχουν στην CERT-ΕΕ ψηφιακές πληροφορίες που δημιουργούνται από τη χρήση ηλεκτρονικών συσκευών που εμπλέκονται στα αντίστοιχα περιστατικά τους. Η CERT-ΕΕ μπορεί να παρέχει περαιτέρω λεπτομερή στοιχεία σχετικά με τα είδη πληροφοριών που χρειάζεται για την επίγνωση της κατάστασης και την αντιμετώπιση περιστατικών.

8. Η CERT-ΕΕ υποβάλλει ανά τρίμηνο στο ΔΣΚ, στον ENISA, στο EU INTCEN και στο δίκτυο CSIRT συνοπτική έκθεση που περιλαμβάνει ανωνυμοποιημένα και συγκεντρωτικά δεδομένα σχετικά με σημαντικά περιστατικά, περιστατικά, κυβερνοαπειλές, παρ' ολίγον περιστατικά και ευπάθειες σύμφωνα με το άρθρο 20 και σημαντικά περιστατικά που κοινοποιούνται σύμφωνα με την παράγραφο 2 του παρόντος άρθρου. Η συνοπτική έκθεση παρέχει στοιχεία για την ανά διετία έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση που εγκρίνεται σύμφωνα με το άρθρο 18 της οδηγίας (ΕΕ) 2022/2555.

9. Έως τις … [6 μήνες από την ημερομηνία έναρξης της ισχύος του παρόντος κανονισμού], το ΔΣΚ εκδίδει κατευθυντήριες γραμμές ή συστάσεις με τις οποίες προσδιορίζει περαιτέρω τις ρυθμίσεις, τον μορφότυπο και το περιεχόμενο της υποβολής εκθέσεων σύμφωνα με το παρόν άρθρο. Κατά την κατάρτιση των εν λόγω κατευθυντήριων γραμμών ή συστάσεων, το ΔΣΚ λαμβάνει υπόψη τυχόν εκτελεστικές πράξεις που εκδίδονται σύμφωνα με το άρθρο 23 παράγραφος 11 της οδηγίας (ΕΕ) 2022/2555 και καθορίζουν το είδος των πληροφοριών, τον μορφότυπο και τη διαδικασία των κοινοποιήσεων. Η CERT-ΕΕ διαδίδει τις κατάλληλες τεχνικές λεπτομέρειες ώστε να διευκολύνει τις οντότητες της Ένωσης στον προδραστικό εντοπισμό, στην αντιμετώπιση περιστατικών ή στην εφαρμογή μέτρων μετριασμού.

10. Οι υποχρεώσεις υποβολής εκθέσεων που ορίζονται στο παρόν άρθρο δεν επεκτείνονται σε:

α) ΔΠΕΕ·

β) πληροφορίες των οποίων η περαιτέρω διανομή έχει αποκλειστεί μέσω ορατής σήμανσης, εκτός εάν έχει επιτραπεί ρητά η κοινοποίησή τους στην CERT-ΕΕ.

Άρθρο 22

Συντονισμός της αντιμετώπισης περιστατικών και σχετική συνεργασία

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 περιστατικά, κυβερνοαπειλές, ευπάθειες και παρ' ολίγον περιστατικά μεταξύ:

α) οντοτήτων της Ένωσης·

β) των ομολόγων που αναφέρονται στα άρθρα 17 και 18.

2. Η CERT-ΕΕ, κατά περίπτωση σε στενή συνεργασία με τον ENISA, διευκολύνει τον συντονισμό μεταξύ των οντοτήτων της Ένωσης για την αντιμετώπιση περιστατικών, μεταξύ άλλων με:

α) συμβολή σε συνεπή εξωτερική επικοινωνία·

β) αμοιβαία στήριξη, μεταξύ άλλων με την ανταλλαγή πληροφοριών χρήσιμων για τις οντότητες της Ένωσης, ή με την παροχή συνδρομής, κατά περίπτωση απευθείας επιτόπου·

γ) βέλτιστη χρήση επιχειρησιακών πόρων·

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

3. Η CERT-ΕΕ, σε στενή συνεργασία με τον ENISA, στηρίζει τις οντότητες της Ένωσης όσον αφορά την επίγνωση της κατάστασης σχετικά με περιστατικά, κυβερνοαπειλές, ευπάθειες και παρ' ολίγον περιστατικά, καθώς και την ανταλλαγή σχετικών εξελίξεων στον τομέα της κυβερνοασφάλειας.

4. Έως τις … [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], το ΔΣΚ εκδίδει, βάσει πρότασης της CERT-ΕΕ, κατευθυντήριες γραμμές ή συστάσεις σχετικά με τον συντονισμό της αντιμετώπισης περιστατικών και τη σχετική 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, χωρίς αδικαιολόγητη καθυστέρηση.

5. Κατόπιν ειδικού αιτήματος κράτους μέλους και με την έγκριση των οικείων οντοτήτων της Ένωσης, η CERT-ΕΕ μπορεί να καλεί εμπειρογνώμονες από τον κατάλογο που αναφέρεται στο άρθρο 23 παράγραφος 4, προκειμένου να συμβάλουν στην αντιμετώπιση σοβαρού περιστατικού που έχει αντίκτυπο στο εν λόγω κράτος μέλος ή περιστατικού μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 15 παράγραφος 3 στοιχείο ζ) της οδηγίας (ΕΕ) 2022/2555. Ειδικοί κανόνες σχετικά με την πρόσβαση και τη χρήση τεχνικών εμπειρογνωμόνων από οντότητες της Ένωσης εγκρίνονται από το ΔΣΚ βάσει πρότασης της CERT ΕΕ.

Άρθρο 23

Διαχείριση σοβαρών περιστατικών

1. Για την υποστήριξη σε επιχειρησιακό επίπεδο της συντονισμένης διαχείρισης σοβαρών περιστατικών που επηρεάζουν οντότητες της Ένωσης και για τη συμβολή στην τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των οντοτήτων της Ένωσης και με τα κράτη μέλη, το ΔΣΚ καταρτίζει, σύμφωνα με το άρθρο 11 στοιχείο ιζ), σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τις δραστηριότητες που αναφέρονται στο άρθρο 22 παράγραφος 2, σε στενή συνεργασία με την CERT-ΕΕ και τον ENISA. Το σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία:

α) ρυθμίσεις σχετικά με τον συντονισμό και τη ροή πληροφοριών μεταξύ των οντοτήτων της Ένωσης για τη διαχείριση σοβαρών περιστατικών σε επιχειρησιακό επίπεδο·

β) κοινές τυποποιημένες επιχειρησιακές διαδικασίες·

γ) κοινή ταξινόμηση της κρισιμότητας των σοβαρών περιστατικών και των σημείων που πυροδοτούν κρίσεις·

δ) τακτικές ασκήσεις·

ε) ασφαλείς διαύλους επικοινωνίας που πρέπει να χρησιμοποιούνται.

2. Ο εκπρόσωπος της Επιτροπής στο ΔΣΚ, με την επιφύλαξη του σχεδίου διαχείρισης κρίσεων στον κυβερνοχώρο που καταρτίζεται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και με την επιφύλαξη του άρθρου 16 παράγραφος 2 πρώτο εδάφιο της οδηγίας (ΕΕ) 2022/2555, αποτελεί το σημείο επαφής για την ανταλλαγή σχετικών πληροφοριών με το EU-CyCLONe σε σχέση με σοβαρά περιστατικά.

3. Η CERT-ΕΕ συντονίζει μεταξύ των οντοτήτων της Ένωσης τη διαχείριση σοβαρών περιστατικών. Τηρεί κατάλογο της διαθέσιμης τεχνικής εμπειρογνωσίας που απαιτείται για την αντιμετώπιση περιστατικών σε περίπτωση σοβαρών περιστατικών και επικουρεί το ΔΣΚ στον συντονισμό των σχεδίων διαχείρισης κρίσεων στον κυβερνοχώρο των οντοτήτων της Ένωσης για σοβαρά περιστατικά που αναφέρονται στο άρθρο 9 παράγραφος 2.

4. Οι οντότητες 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.

Κεφάλαιο VI
Τελικές διατάξεις

Άρθρο 24

Αρχική ανακατανομή των πιστώσεων του προϋπολογισμού

Προκειμένου να διασφαλιστεί η ορθή και σταθερή λειτουργία της CERT-ΕΕ, η Επιτροπή μπορεί να προτείνει την ανακατανομή προσωπικού και οικονομικών πόρων στον προϋπολογισμό της Επιτροπής για χρήση σε επιχειρήσεις της CERT-ΕΕ. Η ανακατανομή τίθεται σε εφαρμογή ταυτόχρονα με τον πρώτο ετήσιο προϋπολογισμό της Ένωσης που θα εγκριθεί μετά την έναρξη ισχύος του παρόντος κανονισμού.

Άρθρο 25

Επανεξέταση

1. Έως τις ... [12 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού], και στη συνέχεια σε ετήσια βάση, το ΔΣΚ, με τη συνδρομή της CERT-ΕΕ, υποβάλλει εκθέσεις στην Επιτροπή σχετικά με την εφαρμογή του παρόντος κανονισμού. Το ΔΣΚ μπορεί να απευθύνει συστάσεις στην Επιτροπή για την επανεξέταση του παρόντος κανονισμού.

2. Έως τις [36 μήνες από την ημερομηνία έναρξης ισχύος του παρόντος κανονισμού] και στη συνέχεια ανά διετία, η Επιτροπή διενεργεί αξιολόγηση και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την εφαρμογή του παρόντος κανονισμού και την πείρα που αποκτήθηκε σε στρατηγικό και επιχειρησιακό επίπεδο.

Η έκθεση που αναφέρεται στο πρώτο εδάφιο της παρούσας παραγράφου περιλαμβάνει την επανεξέταση που αναφέρεται στο άρθρο 16 παράγραφος 1, σχετικά με τη δυνατότητα σύστασης της CERT-ΕΕ ως γραφείου της Ένωσης.

3. Έως τις … [πέντε έτη από την έναρξη ισχύος του παρόντος κανονισμού], 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. Η Επιτροπή αξιολογεί επίσης κατά πόσον είναι σκόπιμο να συμπεριληφθούν τα δικτυακά και πληροφοριακά συστήματα που χειρίζονται ΔΠΕΕ στο πεδίο εφαρμογής του παρόντος κανονισμού, λαμβάνοντας υπόψη άλλες νομοθετικές πράξεις της Ένωσης που εφαρμόζονται στα εν λόγω συστήματα. Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.

Άρθρο 26

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.

Στρασβούργο,

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