2024/1366

24.5.2024

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1366 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 11ης Μαρτίου 2024

για τη συμπλήρωση του κανονισμού (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τη θέσπιση κώδικα δικτύου σχετικά με ειδικούς τομεακούς κανόνες για τις πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την εσωτερική αγορά ηλεκτρικής ενέργειας ([1]), και ιδίως το άρθρο 59 παράγραφος 2 στοιχείο ε),

Εκτιμώντας τα ακόλουθα:

(1) Η διαχείριση κινδύνων για την κυβερνοασφάλεια είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας του εφοδιασμού με ηλεκτρική ενέργεια και για τη διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας.

(2) Η ψηφιοποίηση και η κυβερνοασφάλεια είναι καθοριστικής σημασίας για την παροχή βασικών υπηρεσιών και, ως εκ τούτου, έχουν στρατηγική σημασία για τις κρίσιμες ενεργειακές υποδομές.

(3) Η οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]) καθορίζει μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση. Ο κανονισμός (ΕΕ) 2019/941 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]) συμπληρώνει την οδηγία (ΕΕ) 2022/2555 διασφαλίζοντας ότι τα κυβερνοπεριστατικά στον τομέα της ηλεκτρικής ενέργειας προσδιορίζονται δεόντως ως κίνδυνος και ότι τα μέτρα που λαμβάνονται για την αντιμετώπισή τους περιλαμβάνονται κατάλληλα στα σχέδια ετοιμότητας αντιμετώπισης κινδύνων. Ο κανονισμός (ΕΕ) 2019/943 συμπληρώνει την οδηγία (ΕΕ) 2022/2555 και τον κανονισμό (ΕΕ) 2019/941 με τον καθορισμό ειδικών κανόνων για τον τομέα της ηλεκτρικής ενέργειας σε επίπεδο Ένωσης. Επίσης, ο παρών κατ' εξουσιοδότηση κανονισμός συμπληρώνει τις διατάξεις της οδηγίας (ΕΕ) 2022/2555 σχετικά με τον τομέα της ηλεκτρικής ενέργειας, στις περιπτώσεις που αφορούν τις διασυνοριακές ροές ηλεκτρικής ενέργειας.

(4) Σε ένα πλαίσιο διασυνδεδεμένων ψηφιοποιημένων συστημάτων ηλεκτρικής ενέργειας, η πρόληψη και η διαχείριση κρίσεων ηλεκτρικής ενέργειας που σχετίζονται με κυβερνοεπιθέσεις δεν μπορεί να θεωρηθεί αποκλειστικά εθνικό καθήκον. Θα πρέπει να αναπτυχθούν στο έπακρο αποδοτικότερα και λιγότερο δαπανηρά μέτρα μέσω συνεργασίας σε περιφερειακό και ενωσιακό επίπεδο. Ως εκ τούτου, απαιτείται ένα κοινό πλαίσιο κανόνων και καλύτερα συντονισμένες διαδικασίες προκειμένου να διασφαλιστεί ότι τα κράτη μέλη και άλλοι φορείς μπορούν να συνεργάζονται αποτελεσματικά σε διασυνοριακό επίπεδο, με πνεύμα αυξημένης διαφάνειας, εμπιστοσύνης και αλληλεγγύης μεταξύ των κρατών μελών και των αρμόδιων αρχών που είναι υπεύθυνες για την ηλεκτρική ενέργεια και την κυβερνοασφάλεια.

(5) Για τη διαχείριση των κινδύνων για την κυβερνοασφάλεια στο πλαίσιο του πεδίου εφαρμογής του παρόντος κανονισμού απαιτείται μια διαρθρωμένη διαδικασία που να περιλαμβάνει, μεταξύ άλλων, τον προσδιορισμό των κινδύνων για τις διασυνοριακές ροές ηλεκτρικής ενέργειας που απορρέουν από κυβερνοεπιθέσεις, τις σχετικές επιχειρησιακές διαδικασίες και περιμέτρους, τους αντίστοιχους ελέγχους κυβερνοασφάλειας και μηχανισμούς επαλήθευσης. Παρόλο που το χρονοδιάγραμμα για ολόκληρη τη διαδικασία καλύπτει αρκετά έτη, κάθε στάδιο της διαδικασίας θα πρέπει να συμβάλλει στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας στον τομέα και στον μετριασμό των κινδύνων για την κυβερνοασφάλεια. Όλοι οι συμμετέχοντες στη διαδικασία θα πρέπει να καταβάλουν κάθε δυνατή προσπάθεια για να αναπτύξουν και να συμφωνήσουν μεθοδολογίες το συντομότερο δυνατόν, χωρίς αδικαιολόγητη καθυστέρηση, και, σε κάθε περίπτωση, το αργότερο εντός των προθεσμιών που ορίζονται στον παρόντα κανονισμό.

([1]) ΕΕ L 158 της 14.6.2019, σ. 54.

([2]) 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, 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).

([3]) Κανονισμός (ΕΕ) 2019/941 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με την ετοιμότητα αντιμετώπισης κινδύνων στον τομέα της ηλεκτρικής ενέργειας και με την κατάργηση της οδηγίας 2005/89/ΕΚ (ΕΕ L 158 της 14.6.2019, σ. 1).

(6) Οι εκτιμήσεις κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, κρατών μελών, περιφερειών και οντοτήτων στον παρόντα κανονισμό μπορούν να περιορίζονται σε εκείνες που προκύπτουν από κυβερνοεπιθέσεις, όπως αυτές ορίζονται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), με αποτέλεσμα να εξαιρούνται, για παράδειγμα, υλικές επιθέσεις, φυσικές καταστροφές και διακοπές λειτουργίας λόγω απώλειας εγκαταστάσεων ή ανθρώπινων πόρων. Οι κίνδυνοι σε επίπεδο Ένωσης και οι περιφερειακοί κίνδυνοι που σχετίζονται με υλικές επιθέσεις ή φυσικές καταστροφές στον τομέα της ηλεκτρικής ενέργειας καλύπτονται ήδη από άλλη ισχύουσα νομοθεσία της Ένωσης, όπως το άρθρο 5 του κανονισμού (ΕΕ) 2019/941 ή ο κανονισμός (ΕΕ) 2017/1485 της Επιτροπής ([5]) σχετικά με τον καθορισμό κατευθυντήριων γραμμών για τη λειτουργία του συστήματος μεταφοράς ηλεκτρικής ενέργειας. Ομοίως, η οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]) για την ανθεκτικότητα των κρίσιμων οντοτήτων αποσκοπεί στη μείωση των ευπαθειών και στην ενίσχυση της φυσικής ανθεκτικότητας των κρίσιμων οντοτήτων, και καλύπτει όλους τους σχετικούς φυσικούς και ανθρωπογενείς κινδύνους που ενδέχεται να επηρεάζουν την παροχή βασικών υπηρεσιών, στους οποίους περιλαμβάνονται, μεταξύ άλλων, ατυχήματα, φυσικές καταστροφές, καταστάσεις έκτακτης ανάγκης στον τομέα της δημόσιας υγείας, όπως οι πανδημίες, και υβριδικές απειλές ή άλλες ανταγωνιστικές απειλές, συμπεριλαμβανομένων των τρομοκρατικών εγκλημάτων, της διείσδυσης εγκληματικών στοιχείων και της δολιοφθοράς.

(7) Η έννοια των «οντοτήτων υψηλού αντικτύπου» και των «οντοτήτων κρίσιμου αντικτύπου» στον παρόντα κανονισμό είναι θεμελιώδους σημασίας για τον καθορισμό του φάσματος των οντοτήτων που θα υπόκεινται στις υποχρεώσεις που περιγράφονται στον παρόντα κανονισμό. Η βασιζόμενη στον κίνδυνο προσέγγιση που περιγράφεται στις διάφορες διατάξεις αποσκοπεί στον προσδιορισμό των διαδικασιών, των υποστηρικτικών περιουσιακών στοιχείων και των οντοτήτων που τα διαχειρίζονται, τα οποία επηρεάζουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Ανάλογα με τον βαθμό του αντικτύπου των πιθανών κυβερνοεπιθέσεων στις λειτουργίες τους όσον αφορά τις διασυνοριακές ροές ηλεκτρικής ενέργειας, μπορούν να θεωρηθούν «υψηλού αντικτύπου» ή «κρίσιμου αντικτύπου». Το άρθρο 3 της οδηγίας (ΕΕ) 2022/2555 καθορίζει τις έννοιες των βασικών και σημαντικών οντοτήτων και τα κριτήρια για τον προσδιορισμό των οντοτήτων αυτών των κατηγοριών. Παρόλο που πολλές από αυτές θα θεωρούνται και θα προσδιορίζονται ταυτόχρονα ως «βασικές» κατά την έννοια του άρθρου 3 της οδηγίας (ΕΕ) 2022/2555 και ως υψηλού αντικτύπου ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 του παρόντος κανονισμού, τα κριτήρια που ορίζονται στον παρόντα κανονισμό αναφέρονται μόνο στον ρόλο και στον αντίκτυπό τους στις διαδικασίες ηλεκτρικής ενέργειας που επηρεάζουν τις διασυνοριακές ροές, χωρίς να λαμβάνονται υπόψη τα κριτήρια που ορίζονται στο άρθρο 3 της οδηγίας (ΕΕ) 2022/2555.

(8) Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, οι οποίες θεωρούνται υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 του παρόντος κανονισμού και υπόκεινται στις υποχρεώσεις που ορίζονται σε αυτόν, είναι πρωτίστως εκείνες που έχουν άμεσο αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας στην ΕΕ.

(9) Ο παρών κανονισμός χρησιμοποιεί υφιστάμενους μηχανισμούς και μέσα, τα οποία έχουν ήδη θεσπιστεί με άλλες νομοθετικές πράξεις, για τη διασφάλιση της αποδοτικότητας και την αποφυγή επικαλύψεων στην επίτευξη των στόχων.

(10) Κατά την εφαρμογή του παρόντος κανονισμού, τα κράτη μέλη, οι σχετικές αρχές και οι διαχειριστές συστημάτων θα πρέπει να λαμβάνουν υπόψη τα συμφωνηθέντα ευρωπαϊκά πρότυπα και τις τεχνικές προδιαγραφές των ευρωπαϊκών οργανισμών τυποποίησης και να ενεργούν σύμφωνα με την ενωσιακή νομοθεσία σχετικά με τη διάθεση στην αγορά ή τη θέση σε λειτουργία προϊόντων που καλύπτονται από την εν λόγω ενωσιακή νομοθεσία.

([4]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1).

([5]) Κανονισμός (ΕΕ) 2017/1485 της Επιτροπής, της 2ας Αυγούστου 2017, σχετικά με τον καθορισμό κατευθυντήριων γραμμών για τη λειτουργία του συστήματος μεταφοράς ηλεκτρικής ενέργειας (ΕΕ L 220 της 25.8.2017, σ. 1).

([6]) Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (ΕΕ L 333 της 27.12.2022, σ. 164).

(11) Με σκοπό τον μετριασμό των κινδύνων για την κυβερνοασφάλεια, είναι αναγκαίο να καταρτιστεί λεπτομερές εγχειρίδιο κανόνων που θα διέπει τις δράσεις και τη συνεργασία μεταξύ των σχετικών ενδιαφερόμενων μερών, οι δραστηριότητες των οποίων αφορούν πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας, με στόχο τη διαφύλαξη της ασφάλειας του συστήματος. Οι εν λόγω οργανωτικοί και τεχνικοί κανόνες θα πρέπει να διασφαλίζουν ότι τα περισσότερα περιστατικά στον τομέα της ηλεκτρικής ενέργειας των οποίων τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας αντιμετωπίζονται αποτελεσματικά σε επιχειρησιακό επίπεδο. Είναι αναγκαίο να καθοριστεί τι θα πρέπει να κάνουν τα εν λόγω ενδιαφερόμενα μέρη για την πρόληψη τέτοιων κρίσεων και ποια μέτρα μπορούν να λάβουν σε περίπτωση που οι κανόνες λειτουργίας του συστήματος δεν επαρκούν πια από μόνοι τους. Ως εκ τούτου, είναι αναγκαίο να θεσπιστεί κοινό πλαίσιο κανόνων για τον τρόπο πρόληψης, προετοιμασίας και διαχείρισης ταυτόχρονων κρίσεων ηλεκτρικής ενέργειας των οποίων τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας. Επιτυγχάνεται έτσι μεγαλύτερη διαφάνεια κατά το στάδιο της προετοιμασίας και κατά τη διάρκεια ταυτόχρονης κρίσης ηλεκτρικής ενέργειας και διασφαλίζεται ότι τα μέτρα λαμβάνονται με συντονισμένο και αποτελεσματικό τρόπο από κοινού με τις αρμόδιες για την κυβερνοασφάλεια αρχές στα κράτη μέλη. Τα κράτη μέλη και οι σχετικές οντότητες θα πρέπει να υποχρεούνται να συνεργάζονται, σε περιφερειακό επίπεδο και, κατά περίπτωση, διμερώς, σε πνεύμα αλληλεγγύης. Η εν λόγω συνεργασία και οι εν λόγω κανόνες αποσκοπούν στη βελτίωση της ετοιμότητας αντιμετώπισης κινδύνων στον τομέα της κυβερνοασφάλειας με χαμηλότερο κόστος, σύμφωνα επίσης με τους στόχους της οδηγίας (ΕΕ) 2022/2555. Κρίνεται επίσης αναγκαίο να ενδυναμωθεί η εσωτερική αγορά ηλεκτρικής ενέργειας με την ενίσχυση της εμπιστοσύνης μεταξύ των κρατών μελών, ιδίως με τον μετριασμό του κινδύνου αδικαιολόγητης περικοπής των διασυνοριακών ροών ηλεκτρικής ενέργειας, με αποτέλεσμα να μειώνεται ο κίνδυνος αρνητικών δευτερογενών επιπτώσεων στα γειτονικά κράτη μέλη.

(12) Η ασφάλεια του εφοδιασμού με ηλεκτρική ενέργεια συνεπάγεται αποτελεσματική συνεργασία μεταξύ κρατών μελών, θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, και σχετικών ενδιαφερόμενων μερών. Οι διαχειριστές συστημάτων διανομής και οι διαχειριστές συστημάτων μεταφοράς διαδραματίζουν καίριο ρόλο στην κατοχύρωση ενός ασφαλούς, αξιόπιστου και αποδοτικού συστήματος ηλεκτρικής ενέργειας, σύμφωνα με τα άρθρα 31 και 40 της οδηγίας (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]). Οι διάφορες ρυθμιστικές αρχές και άλλες σχετικές αρμόδιες εθνικές αρχές διαδραματίζουν επίσης σημαντικό ρόλο στη διασφάλιση και την παρακολούθηση της κυβερνοασφάλειας στο πλαίσιο του εφοδιασμού με ηλεκτρική ενέργεια, ως μέρος των καθηκόντων που τους ανατίθενται με τις οδηγίες (ΕΕ) 2019/944 και (ΕΕ) 2022/2555. Τα κράτη μέλη θα πρέπει να ορίσουν υφιστάμενη ή νέα οντότητα ως οικεία αρμόδια εθνική αρχή για την εφαρμογή του παρόντος κανονισμού, με στόχο τη διασφάλιση της διαφανούς και συμπεριληπτικής συμμετοχής όλων των εμπλεκόμενων παραγόντων, την αποδοτική προετοιμασία και ορθή εφαρμογή του, τη συνεργασία μεταξύ των διαφόρων σχετικών ενδιαφερόμενων μερών και αρμόδιων αρχών στον τομέα της ηλεκτρικής ενέργειας και της κυβερνοασφάλειας, καθώς και τη διευκόλυνση της πρόληψης και της εκ των υστέρων αξιολόγησης των κρίσεων ηλεκτρικής ενέργειας των οποίων τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας, καθώς και της ανταλλαγής πληροφοριών σε σχέση με αυτές.

(13) Όταν μια οντότητα υψηλού ή κρίσιμου αντικτύπου παρέχει υπηρεσίες σε περισσότερα από ένα κράτη μέλη, ή έχει την έδρα της ή άλλη εγκατάσταση ή εκπρόσωπο σε κράτος μέλος, αλλά τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε ένα ή περισσότερα άλλα κράτη μέλη, τα εν λόγω κράτη μέλη θα πρέπει να ενθαρρύνουν τις οικείες αντίστοιχες αρμόδιες αρχές να προβαίνουν σε κάθε δυνατή προσπάθεια για να συνεργάζονται και να αλληλοβοηθούνται, ανάλογα με τις ανάγκες.

(14) Τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν τις αναγκαίες εξουσίες, όσον αφορά τις οντότητες υψηλού ή κρίσιμου αντικτύπου, για την προώθηση της συμμόρφωσης με τον παρόντα κανονισμό. Οι εν λόγω εξουσίες θα πρέπει να παρέχουν στις αρμόδιες αρχές τη δυνατότητα να διενεργούν επιτόπιες επιθεωρήσεις και εποπτεία εκτός των εγκαταστάσεων. Αυτό μπορεί να περιλαμβάνει τυχαίους ελέγχους, διενέργεια τακτικών ελέγχων, στοχευμένους ελέγχους ασφάλειας με βάση εκτιμήσεις κινδύνου ή διαθέσιμες πληροφορίες που σχετίζονται με τον κίνδυνο και σαρώσεις ασφάλειας, βάσει αντικειμενικών, μη διακρισιακών, δίκαιων και διαφανών κριτηρίων εκτίμησης κινδύνων, συμπεριλαμβανομένης της υποβολής αιτημάτων για πληροφορίες που είναι αναγκαίες για την αξιολόγηση των μέτρων κυβερνοασφάλειας που λαμβάνει η οντότητα. Οι εν λόγω πληροφορίες θα πρέπει να περιλαμβάνουν τεκμηριωμένες πολιτικές κυβερνοασφάλειας, δεδομένα πρόσβασης, έγγραφα ή οποιεσδήποτε πληροφορίες είναι απαραίτητες για την εκτέλεση των εποπτικών καθηκόντων τους, καθώς και αποδεικτικά στοιχεία για την εφαρμογή πολιτικών κυβερνοασφάλειας, όπως τα αποτελέσματα ελέγχων ασφάλειας που διενεργούνται από ειδικευμένο ελεγκτή και τα αντίστοιχα υποκείμενα αποδεικτικά στοιχεία.

([7]) Οδηγία (ΕΕ) 2019/944 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και την τροποποίηση της οδηγίας 2012/27/ΕΕ (ΕΕ L 158 της 14.6.2019, σ. 125).

(15) Προκειμένου να αποφεύγονται κενά ή αλληλεπικαλύψεις μεταξύ των υποχρεώσεων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που επιβάλλονται στις οντότητες υψηλού ή κρίσιμου αντικτύπου, οι εθνικές αρχές βάσει της οδηγίας (ΕΕ) 2022/2555 και οι αρμόδιες αρχές βάσει του παρόντος κανονισμού θα πρέπει να συνεργάζονται σχετικά με την εφαρμογή μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και την εποπτεία της συμμόρφωσης με τα εν λόγω μέτρα σε εθνικό επίπεδο. Η συμμόρφωση μιας οντότητας με τις απαιτήσεις διαχείρισης κινδύνων για την κυβερνοασφάλεια που ορίζονται στον παρόντα κανονισμό θα μπορούσε να θεωρηθεί από τις αρμόδιες αρχές, βάσει της οδηγίας (ΕΕ) 2022/2555, ότι διασφαλίζει τη συμμόρφωση με τις αντίστοιχες απαιτήσεις που ορίζονται στην εν λόγω οδηγία, ή αντιστρόφως.

(16) Για να υπάρξει μια κοινή προσέγγιση για την πρόληψη και τη διαχείριση ταυτόχρονων κρίσεων ηλεκτρικής ενέργειας απαιτείται κοινή αντίληψη μεταξύ των κρατών μελών ως προς το τι συνιστά ταυτόχρονη κρίση ηλεκτρικής ενέργειας και πότε μια κυβερνοεπίθεση αποτελεί σημαντικό παράγοντα. Ειδικότερα, θα πρέπει να διευκολυνθεί ο συντονισμός μεταξύ των κρατών μελών και των σχετικών οντοτήτων με σκοπό την αντιμετώπιση μιας κατάστασης στην οποία υπάρχει ή επίκειται δυνητικός κίνδυνος σημαντικής έλλειψης ηλεκτρικής ενέργειας ή αδυναμίας παροχής ηλεκτρικής ενέργειας σε πελάτες, λόγω κυβερνοεπίθεσης.

(17) Η αιτιολογική σκέψη 1 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) αναγνωρίζει τον ζωτικό ρόλο των συστημάτων δικτύου και πληροφοριών και των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών για τη διατήρηση της λειτουργίας της οικονομίας σε βασικούς τομείς όπως η ενέργεια, ενώ η αιτιολογική σκέψη 44 εξηγεί ότι ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA) θα πρέπει να συνεργάζεται με τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία των Ρυθμιστικών Αρχών Ενέργειας (στο εξής: ACER).

(18) Ο κανονισμός (ΕΕ) 2019/943 αναθέτει ειδικές αρμοδιότητες όσον αφορά την κυβερνοασφάλεια στους διαχειριστές συστημάτων μεταφοράς (στο εξής: ΔΣΜ) και στους διαχειριστές συστημάτων διανομής (στο εξής: ΔΣΔ). Οι ευρωπαϊκές ενώσεις τους, δηλαδή το ευρωπαϊκό δίκτυο ΔΣΜ ηλεκτρικής ενέργειας (στο εξής: ΕΔΔΣΜ ηλεκτρικής ενέργειας) και ο ευρωπαϊκός φορέας ΔΣΔ (στο εξής: φορέας ΔΣΔ της ΕΕ), προωθούν, σύμφωνα με τα άρθρα 30 και 55 του εν λόγω κανονισμού, αντίστοιχα, την κυβερνοασφάλεια σε συνεργασία με τις αρμόδιες αρχές και τις ρυθμιζόμενες οντότητες.

(19) Για να υπάρξει μια κοινή προσέγγιση για την πρόληψη και τη διαχείριση ταυτόχρονων κρίσεων ηλεκτρικής ενέργειας των οποίων τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας, όλα τα σχετικά ενδιαφερόμενα μέρη πρέπει να χρησιμοποιούν εναρμονισμένες μεθόδους και ορισμούς για τον προσδιορισμό των κινδύνων που σχετίζονται με την κυβερνοασφάλεια του εφοδιασμού με ηλεκτρική ενέργεια. Πρέπει επίσης να είναι σε θέση να συγκρίνουν αποτελεσματικά τις επιδόσεις τόσο των ίδιων όσο και των γειτόνων τους στον εν λόγω τομέα. Ως εκ τούτου, είναι αναγκαίο να καθοριστούν οι διαδικασίες, οι ρόλοι και οι αρμοδιότητες για την ανάπτυξη και την επικαιροποίηση μεθοδολογιών διαχείρισης κινδύνου, κλιμάκων ταξινόμησης περιστατικών και μέτρων κυβερνοασφάλειας προσαρμοσμένων στους κινδύνους για την κυβερνοασφάλεια που επηρεάζουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας.

(20) Τα κράτη μέλη, μέσω της αρμόδιας αρχής που ορίζεται για τον παρόντα κανονισμό, είναι υπεύθυνα να προσδιορίσουν τις οντότητες που πληρούν τα κριτήρια για να χαρακτηριστούν οντότητες υψηλού ή κρίσιμου αντικτύπου. Προκειμένου να εξαλειφθούν οι αποκλίσεις μεταξύ των κρατών μελών ως προς το θέμα αυτό και να διασφαλιστεί για όλες τις σχετικές οντότητες ασφάλεια δικαίου όσον αφορά τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών, θα πρέπει να θεσπιστεί ένα σύνολο κριτηρίων για τον προσδιορισμό των οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού. Το εν λόγω σύνολο κριτηρίων θα πρέπει να καθοριστεί και να επικαιροποιείται τακτικά μέσω της διαδικασίας ανάπτυξης και έγκρισης όρων, προϋποθέσεων και μεθοδολογιών που καθορίζονται στον παρόντα κανονισμό.

(21) Οι διατάξεις του παρόντος κανονισμού δεν θα πρέπει να θίγουν το ενωσιακό δίκαιο που προβλέπει συγκεκριμένους κανόνες για την πιστοποίηση προϊόντων τεχνολογίας πληροφοριών και επικοινωνιών (στο εξής: ΤΠΕ), υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, ιδίως δεν θα πρέπει να θίγουν τον κανονισμό (ΕΕ) 2019/881 όσον αφορά το πλαίσιο για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας. Στο πλαίσιο του παρόντος κανονισμού, τα προϊόντα ΤΠΕ θα πρέπει επίσης να περιλαμβάνουν τεχνικές συσκευές και λογισμικό που καθιστούν δυνατή την άμεση αλληλεπίδραση με το ηλεκτροτεχνικό δίκτυο, ιδίως βιομηχανικά συστήματα ελέγχου που μπορούν να χρησιμοποιηθούν για τη μεταφορά ενέργειας, τη διανομή ενέργειας και την παραγωγή ενέργειας, καθώς και για τη συλλογή και τη διαβίβαση σχετικών πληροφοριών. Οι διατάξεις θα πρέπει να διασφαλίζουν ότι οι σχετικοί στόχοι ασφάλειας του άρθρου 51 του κανονισμού (ΕΕ) 2019/881 επιτυγχάνονται από τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ και τις διαδικασίες ΤΠΕ που αποτελούν αντικείμενο δημόσιας σύμβασης.

([8]) 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).

(22) Οι πρόσφατες κυβερνοεπιθέσεις δείχνουν ότι οι οντότητες καθίστανται όλο και περισσότερο στόχος επιθέσεων στην αλυσίδα εφοδιασμού. Οι εν λόγω επιθέσεις στην αλυσίδα εφοδιασμού όχι μόνο έχουν αντίκτυπο σε μεμονωμένες οντότητες που εμπίπτουν στο πεδίο εφαρμογής, αλλά μπορούν επίσης να έχουν αλυσιδωτές επιπτώσεις σε μεγαλύτερες επιθέσεις κατά οντοτήτων με τις οποίες είναι συνδεδεμένες στο δίκτυο ηλεκτρικής ενέργειας. Ως εκ τούτου, έχουν προστεθεί διατάξεις και συστάσεις για τον μετριασμό των κινδύνων για την κυβερνοασφάλεια που συνδέονται με διαδικασίες που σχετίζονται με την αλυσίδα εφοδιασμού, ιδίως τις διαδικασίες σύναψης δημόσιων συμβάσεων, οι οποίες έχουν αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας.

(23) Δεδομένου ότι η εκμετάλλευση ευπαθειών στα συστήματα δικτύου και πληροφοριών μπορεί να προκαλέσει σημαντικές ενεργειακές διαταραχές και ζημιά στην οικονομία και στους καταναλωτές, οι εν λόγω ευπάθειες θα πρέπει να εντοπίζονται και να διορθώνονται γρήγορα προκειμένου να μειώνονται οι κίνδυνοι. Για να διευκολυνθεί η αποτελεσματική εφαρμογή του παρόντος κανονισμού, οι σχετικές οντότητες και οι αρμόδιες αρχές θα πρέπει να συνεργάζονται για την άσκηση και τη δοκιμή δραστηριοτήτων που θεωρούνται κατάλληλες για τον σκοπό αυτόν, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών σχετικά με κυβερνοαπειλές, κυβερνοεπιθέσεις, ευπάθειες, εργαλεία και μεθόδους, τακτικές, τεχνικές και διαδικασίες, ετοιμότητα διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας και άλλες ασκήσεις. Καθώς η τεχνολογία εξελίσσεται συνεχώς και η ψηφιοποίηση του τομέα της ηλεκτρικής ενέργειας προχωρά με ταχείς ρυθμούς, η εφαρμογή των διατάξεων που θεσπίζονται δεν θα πρέπει να είναι επιζήμια για την καινοτομία και δεν θα πρέπει να αποτελεί εμπόδιο για την πρόσβαση στην αγορά ηλεκτρικής ενέργειας και την επακόλουθη χρήση καινοτόμων λύσεων που συμβάλλουν στην αποδοτικότητα και στη βιωσιμότητα του συστήματος ηλεκτρικής ενέργειας.

(24) Οι πληροφορίες που συλλέγονται με σκοπό την παρακολούθηση της εφαρμογής του παρόντος κανονισμού θα πρέπει να περιορίζονται εύλογα με βάση την αρχή της ανάγκης για γνώση. Τα ενδιαφερόμενα μέρη θα πρέπει να διαθέτουν εφικτές και αποτελεσματικές προθεσμίες για την υποβολή των εν λόγω πληροφοριών. Θα πρέπει να αποφεύγεται η διπλή κοινοποίηση.

(25) Η προστασία της κυβερνοασφάλειας δεν σταματά στα σύνορα της Ένωσης. Για ένα ασφαλές σύστημα, απαιτείται η συμμετοχή γειτονικών τρίτων χωρών. Η Ένωση και τα κράτη μέλη της θα πρέπει να προσπαθούν να υποστηρίζουν γειτονικές τρίτες χώρες των οποίων οι υποδομές ηλεκτρικής ενέργειας είναι συνδεδεμένες με το ευρωπαϊκό δίκτυο κατά την εφαρμογή παρόμοιων κανόνων κυβερνοασφάλειας όπως αυτών που ορίζονται στον παρόντα κανονισμό.

(26) Προκειμένου να βελτιωθεί εγκαίρως ο συντονισμός σε θέματα ασφάλειας, να δοκιμαστούν μελλοντικοί δεσμευτικοί όροι, προϋποθέσεις και μεθοδολογίες, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, ο φορέας ΔΣΔ της ΕΕ και οι αρμόδιες αρχές θα πρέπει να αρχίσουν να εκπονούν μη δεσμευτική καθοδήγηση αμέσως μετά την έναρξη ισχύος του παρόντος κανονισμού. Η εν λόγω καθοδήγηση θα χρησιμεύσει ως βάση για την ανάπτυξη των μελλοντικών όρων, προϋποθέσεων και μεθοδολογιών. Παράλληλα, οι αρμόδιες αρχές θα πρέπει να προσδιορίσουν οντότητες ως υποψήφιες για να χαρακτηριστούν οντότητες υψηλού ή κρίσιμου αντικτύπου, προκειμένου αυτές να αρχίσουν, σε εθελοντική βάση, να εκπληρώνουν τις υποχρεώσεις τους.

(27) Ο παρών κανονισμός εκπονήθηκε σε στενή συνεργασία με τον ACER, τον ENISA, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, τον φορέα ΔΣΔ της ΕΕ και άλλα ενδιαφερόμενα μέρη, προκειμένου να θεσπιστούν αποτελεσματικοί, ισορροπημένοι και αναλογικοί κανόνες με διαφάνεια και συμμετοχική διαδικασία.

(28) Ο παρών κανονισμός συμπληρώνει και ενισχύει τα μέτρα διαχείρισης κρίσεων που θεσπίστηκαν με το ενωσιακό πλαίσιο αντιμετώπισης κρίσεων κυβερνοασφάλειας, όπως ορίζεται στη σύσταση (ΕΕ) 2017/1584 της Επιτροπής ([9]). Μια κυβερνοεπίθεση θα μπορούσε επίσης να προκαλέσει, να συμβάλει ή να συμπέσει με κρίση ηλεκτρικής ενέργειας, όπως ορίζεται στο άρθρο 2 σημείο 9) του κανονισμού (ΕΕ) 2019/941, επηρεάζοντας τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η εν λόγω κρίση ηλεκτρικής ενέργειας θα μπορούσε να επιφέρει ταυτόχρονη κρίση ηλεκτρικής ενέργειας, όπως ορίζεται στο άρθρο 2 σημείο 10) του κανονισμού (ΕΕ) 2019/941. Ένα τέτοιο περιστατικό θα μπορούσε επίσης να έχει αντίκτυπο σε άλλους τομείς που εξαρτώνται από την ασφάλεια του εφοδιασμού με ηλεκτρική ενέργεια. Σε περίπτωση που ένα τέτοιο περιστατικό εξελιχθεί σε κυβερνοπεριστατικό μεγάλης κλίμακας κατά την έννοια του άρθρου 16 της οδηγίας (ΕΕ) 2022/2555, θα πρέπει να εφαρμόζονται οι διατάξεις του εν λόγω άρθρου για τη σύσταση του ευρωπαϊκού δικτύου οργανώσεων διασύνδεσης για κρίσεις στον κυβερνοχώρο (στο εξής: EU-CyCLONe). Για τη διαχείριση κρίσεων σε επίπεδο Ένωσης, τα ενδιαφερόμενα μέρη θα πρέπει να βασίζονται στις ολοκληρωμένες ρυθμίσεις της ΕΕ για την πολιτική αντιμετώπιση κρίσεων (ρυθμίσεις IPCR) δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 του Συμβουλίου ([10]).

(29) Ο παρών κανονισμός δεν θίγει τη δυνατότητα των κρατών μελών να λαμβάνουν τα αναγκαία μέτρα για την προστασία των ουσιωδών συμφερόντων της ασφάλειάς τους, τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων, σε συμμόρφωση με το δίκαιο της Ένωσης. Σύμφωνα με το άρθρο 346 της ΣΛΕΕ, κανένα κράτος μέλος δεν πρέπει να υποχρεώνεται να παρέχει πληροφορίες, τη διάδοση των οποίων θεωρεί αντίθετη προς τα ουσιώδη συμφέροντα ασφάλειάς του.

([9]) 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).

([10]) Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ολοκληρωμένες ρυθμίσεις της ΕΕ για την πολιτική αντιμετώπιση κρίσεων (ΕΕ L 320 της 17.12.2018, σ. 28).

(30) Μολονότι ο παρών κανονισμός εφαρμόζεται, καταρχήν, σε οντότητες που ασκούν δραστηριότητες στον τομέα της παραγωγής ηλεκτρικής ενέργειας από πυρηνικούς σταθμούς, ορισμένες από τις εν λόγω δραστηριότητες μπορεί να συνδέονται με την εθνική ασφάλεια.

(31) Το δίκαιο της Ένωσης για την προστασία των δεδομένων και το δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας θα πρέπει να εφαρμόζονται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού. Ειδικότερα, ο παρών κανονισμός εφαρμόζεται με την επιφύλαξη του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]), της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]) και του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]). Κατά συνέπεια, ο παρών κανονισμός δεν θα πρέπει να θίγει, μεταξύ άλλων, τα καθήκοντα και τις εξουσίες των αρχών που είναι αρμόδιες για την παρακολούθηση της συμμόρφωσης με το εφαρμοστέο δίκαιο της Ένωσης για την προστασία των δεδομένων και το εφαρμοστέο δίκαιο της Ένωσης για την προστασία της ιδιωτικότητας.

(32) Δεδομένης της σημασίας της διεθνούς συνεργασίας στον τομέα της κυβερνοασφάλειας, οι αρμόδιες αρχές που είναι υπεύθυνες για την εκτέλεση των καθηκόντων που τους ανατίθενται δυνάμει του παρόντος κανονισμού και ορίζονται από τα κράτη μέλη θα πρέπει να είναι σε θέση να συμμετέχουν σε διεθνή δίκτυα συνεργασίας. Ως εκ τούτου, για τους σκοπούς της εκτέλεσης των καθηκόντων τους, οι αρμόδιες αρχές θα πρέπει να είναι σε θέση να ανταλλάσσουν πληροφορίες, συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα, με τις αρμόδιες αρχές τρίτων χωρών, υπό την προϋπόθεση ότι πληρούνται οι προϋποθέσεις, βάσει του δικαίου της Ένωσης για την προστασία των δεδομένων, για διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, συμπεριλαμβανομένων όσων προβλέπονται στο άρθρο 49 του κανονισμού (ΕΕ) 2016/679.

(33) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αναγκαία και αναλογική για τον σκοπό της προστασίας της ασφάλειας περιουσιακών στοιχείων από οντότητες υψηλού ή κρίσιμου αντικτύπου, θα μπορούσε να θεωρηθεί σύννομη λόγω του ότι η εν λόγω επεξεργασία συμμορφώνεται με νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, σύμφωνα με τις απαιτήσεις του άρθρου 6 παράγραφος 1 στοιχείο γ) και του άρθρου 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί επίσης να είναι απαραίτητη για την εξυπηρέτηση έννομων συμφερόντων που επιδιώκονται από οντότητες υψηλού ή κρίσιμου αντικτύπου, καθώς και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας που ενεργούν για λογαριασμό των εν λόγω οντοτήτων, σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ) του κανονισμού (ΕΕ) 2016/679, μεταξύ άλλων όταν η εν λόγω επεξεργασία είναι απαραίτητη για ρυθμίσεις ανταλλαγής πληροφοριών για την κυβερνοασφάλεια ή για την εθελούσια κοινοποίηση σχετικών πληροφοριών σύμφωνα με τον παρόντα κανονισμό. Μέτρα σχετικά με την πρόληψη, την ανίχνευση, τον προσδιορισμό, τον περιορισμό, την ανάλυση και την αντιμετώπιση κυβερνοεπιθέσεων, μέτρα για την ευαισθητοποίηση σχετικά με συγκεκριμένες κυβερνοαπειλές, την ανταλλαγή πληροφοριών στο πλαίσιο της αποκατάστασης ευπαθειών και της συντονισμένης γνωστοποίησης ευπαθειών, την εθελούσια ανταλλαγή πληροφοριών σχετικά με τις εν λόγω κυβερνοεπιθέσεις, κυβερνοαπειλές και ευπάθειες, τους δείκτες παραβίασης, τις τακτικές, τις τεχνικές και τις διαδικασίες, τις ειδοποιήσεις επαγρύπνησης για την κυβερνοασφάλεια και τα εργαλεία διαμόρφωσης ενδέχεται να απαιτούν την επεξεργασία ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως διευθύνσεων IP, ομοιόμορφων εντοπιστών πόρων (URL), ονομάτων τομέα, διευθύνσεων ηλεκτρονικού ταχυδρομείου, και, στον βαθμό που αυτές αποκαλύπτουν δεδομένα προσωπικού χαρακτήρα, χρονοσφραγίδων. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές, ενιαία σημεία επαφής και ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT) ενδέχεται να συνιστά νομική υποχρέωση ή να θεωρείται αναγκαία για την εκτέλεση καθήκοντος δημοσίου συμφέροντος ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο γ) ή ε) και το άρθρο 6 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679, ή για την επιδίωξη έννομου συμφέροντος των οντοτήτων υψηλού ή κρίσιμου αντικτύπου, όπως αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του εν λόγω κανονισμού. Επιπλέον, το εθνικό δίκαιο ενδέχεται να θεσπίζει κανόνες που να επιτρέπουν στις αρμόδιες αρχές, στα ενιαία σημεία επαφής και στις CSIRT, στον βαθμό που είναι αναγκαίο και αναλογικό για τον σκοπό της προστασίας της ασφάλειας των συστημάτων δικτύου και πληροφοριών οντοτήτων υψηλού ή κρίσιμου αντικτύπου, να επεξεργάζονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα σύμφωνα με το άρθρο 9 του κανονισμού (ΕΕ) 2016/679, ιδίως με την πρόβλεψη κατάλληλων και ειδικών μέτρων για τη διασφάλιση των θεμελιωδών δικαιωμάτων και συμφερόντων των φυσικών προσώπων, συμπεριλαμβανομένων τεχνικών περιορισμών στην περαιτέρω χρήση των εν λόγω δεδομένων και της χρήσης προηγμένων μέτρων ασφάλειας και προστασίας της ιδιωτικότητας, όπως η ψευδωνυμοποίηση ή η κρυπτογράφηση όταν η ανωνυμοποίηση μπορεί να επηρεάσει σημαντικά τον επιδιωκόμενο σκοπό.

([11]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([12]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

([13]) 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).

(34) Ως αποτέλεσμα κυβερνοεπιθέσεων, σε πολλές περιπτώσεις διακυβεύονται δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, οι αρμόδιες αρχές θα πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για όλα τα σχετικά θέματα με τις αρχές που αναφέρονται στον κανονισμό (ΕΕ) 2016/679 και στην οδηγία 2002/58/ΕΚ.

(35) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725, η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος και γνωμοδότησε στις 17 Νοεμβρίου 2023,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο

Ο παρών κανονισμός θεσπίζει κώδικα δικτύου ο οποίος καθορίζει ειδικούς τομεακούς κανόνες για τις πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας, συμπεριλαμβανομένων κανόνων για τις κοινές ελάχιστες απαιτήσεις, τον προγραμματισμό, την παρακολούθηση, την υποβολή εκθέσεων και τη διαχείριση κρίσεων.

Άρθρο 2

Πεδίο εφαρμογής

1. Ο παρών κανονισμός εφαρμόζεται στις πτυχές της κυβερνοασφάλειας των διασυνοριακών ροών ηλεκτρικής ενέργειας στις δραστηριότητες των ακόλουθων οντοτήτων, εάν χαρακτηρίζονται ως οντότητες υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24:

α) επιχειρήσεις ηλεκτρικής ενέργειας, όπως ορίζονται στο άρθρο 2 σημείο 57) της οδηγίας (ΕΕ) 2019/944·

β) ορισθέντες διαχειριστές αγοράς ηλεκτρικής ενέργειας (ΝΕΜΟ), όπως ορίζονται στο άρθρο 2 σημείο 8) του κανονισμού (ΕΕ) 2019/943·

γ) οργανωμένες αγορές, όπως ορίζονται στο άρθρο 2 σημείο 4) του εκτελεστικού κανονισμού (ΕΕ) αριθ. 1348/2014 της Επιτροπής ([14]), οι οποίες διεκπεραιώνουν συναλλαγές σε προϊόντα που σχετίζονται με διασυνοριακές ροές ηλεκτρικής ενέργειας·

δ) πάροχοι κρίσιμων υπηρεσιών ΤΠΕ, όπως αναφέρονται στο άρθρο 3 σημείο 9) του παρόντος κανονισμού·

ε) το ΕΔΔΣΜ ηλεκτρικής ενέργειας που συστάθηκε σύμφωνα με το άρθρο 28 του κανονισμού (ΕΕ) 2019/943·

στ) ο φορέας ΔΣΔ της ΕΕ που συστάθηκε σύμφωνα με το άρθρο 52 του κανονισμού (ΕΕ) 2019/943·

ζ) συμβαλλόμενα μέρη με ευθύνη εξισορρόπησης, όπως ορίζονται στο άρθρο 2 σημείο 14) του κανονισμού (ΕΕ) 2019/943·

η) διαχειριστές σημείων επαναφόρτισης, όπως ορίζονται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555·

θ) περιφερειακά συντονιστικά κέντρα (RCC) που έχουν συσταθεί σύμφωνα με το άρθρο 35 του κανονισμού (ΕΕ) 2019/943·

ι) πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας (MSSP), όπως ορίζονται στο άρθρο 6 σημείο 40) της οδηγίας (ΕΕ) 2022/2555·

ια) οποιαδήποτε άλλη οντότητα ή τρίτο μέρος στο οποίο έχουν εκχωρηθεί ή ανατεθεί αρμοδιότητες σύμφωνα με τον παρόντα κανονισμό.

2. Οι ακόλουθες αρχές είναι, στο πλαίσιο της τρέχουσας εντολής τους, υπεύθυνες για την εκτέλεση καθηκόντων που ανατίθενται με τον παρόντα κανονισμό:

α) ο Οργανισμός της Ευρωπαϊκής Ένωσης για τη Συνεργασία των Ρυθμιστικών Αρχών Ενέργειας (ACER), ο οποίος ιδρύθηκε με τον κανονισμό (ΕΕ) 2019/942 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([15])·

β) εθνικές αρμόδιες αρχές που είναι υπεύθυνες για την εκτέλεση των καθηκόντων που τους ανατίθενται δυνάμει του παρόντος κανονισμού και ορίζονται από τα κράτη μέλη σύμφωνα με το άρθρο 4, ή «αρμόδια αρχή»·

γ) εθνικές ρυθμιστικές αρχές τις οποίες ορίζει κάθε κράτος μέλος σύμφωνα με το άρθρο 57 παράγραφος 1 της οδηγίας (ΕΕ) 2019/944·

([14]) Εκτελεστικός κανονισμός (ΕΕ) αριθ. 1348/2014 της Επιτροπής, της 17ης Δεκεμβρίου 2014, σχετικά με την αναφορά δεδομένων για την εφαρμογή του άρθρου 8 παράγραφοι 2 και 6 του κανονισμού (ΕΕ) αριθ. 1227/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την ακεραιότητα και τη διαφάνεια στη χονδρική αγορά ενέργειας (ΕΕ L 363 της 18.12.2014, σ. 121).

([15]) Κανονισμός (ΕΕ) 2019/942 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Ιουνίου 2019, για την ίδρυση Οργανισμού της Ευρωπαϊκής Ένωσης για τη Συνεργασία των Ρυθμιστικών Αρχών Ενέργειας (ΕΕ L 158 της 14.6.2019, σ. 22).

δ) αρχές αρμόδιες για την ετοιμότητα αντιμετώπισης κινδύνων (στο εξής: ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων), οι οποίες έχουν συσταθεί σύμφωνα με το άρθρο 3 του κανονισμού (ΕΕ) 2019/941·

ε) ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT), όπως ορίζονται ή συστήνονται σύμφωνα με το άρθρο 10 της οδηγίας (ΕΕ) 2022/2555·

στ) αρμόδιες αρχές υπεύθυνες για την κυβερνοασφάλεια (στο εξής: ΕΑΑ κυβερνοασφάλειας), όπως ορίζονται ή συστήνονται σύμφωνα με το άρθρο 8 της οδηγίας (ΕΕ) 2022/2555·

ζ) ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο οποίος συστάθηκε δυνάμει του κανονισμού (ΕΕ) 2019/881·

η) οποιαδήποτε άλλη αρχή ή τρίτο μέρος στο οποίο έχουν εκχωρηθεί ή ανατεθεί αρμοδιότητες σύμφωνα με το άρθρο 4 παράγραφος 3.

3. Ο παρών κανονισμός εφαρμόζεται επίσης σε όλες τις οντότητες που δεν είναι εγκατεστημένες στην Ένωση αλλά παρέχουν υπηρεσίες σε οντότητες εντός της Ένωσης, υπό την προϋπόθεση ότι έχουν χαρακτηριστεί από τις αρμόδιες αρχές ως οντότητες υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 2.

4. Ο παρών κανονισμός εφαρμόζεται με την επιφύλαξη της ευθύνης των κρατών μελών για τη διαφύλαξη της εθνικής ασφάλειας και του κυριαρχικού τους δικαιώματος να διαφυλάσσουν άλλες ουσιώδεις λειτουργίες του κράτους, συμπεριλαμβανομένων της διασφάλισης της εδαφικής ακεραιότητας του κράτους και της διατήρησης της δημόσιας τάξης.

5. Ο παρών κανονισμός δεν θίγει την αρμοδιότητα των κρατών μελών να διαφυλάσσουν την εθνική ασφάλεια όσον αφορά τις δραστηριότητες παραγωγής ηλεκτρικής ενέργειας από πυρηνικούς σταθμούς ηλεκτροπαραγωγής, συμπεριλαμβανομένων των δραστηριοτήτων εντός της αξιακής αλυσίδας της πυρηνικής ενέργειας, σύμφωνα με τις Συνθήκες.

6. Οι οντότητες, οι αρμόδιες αρχές, τα ενιαία σημεία επαφής σε επίπεδο οντότητας και οι CSIRT επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στον βαθμό που είναι αναγκαίο για τους σκοπούς του παρόντος κανονισμού και σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, ειδικότερα δε η εν λόγω επεξεργασία βασίζεται στο άρθρο 6 του εν λόγω κανονισμού.

Άρθρο 3

Ορισμοί

Ισχύουν οι ακόλουθοι ορισμοί:

1) «περιουσιακό στοιχείο»: κάθε πληροφορία, λογισμικό ή υλισμικό στα συστήματα δικτύου και πληροφοριών, είτε ενσώματο είτε άυλο, που έχει αξία για ένα άτομο, έναν οργανισμό ή μια κυβέρνηση·

2) «αρμόδια αρχή για την ετοιμότητα αντιμετώπισης κινδύνων»: η αρμόδια αρχή που έχει οριστεί σύμφωνα με το άρθρο 3 του κανονισμού (ΕΕ) 2019/941·

3) «ομάδα αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές»: ομάδα υπεύθυνη για τον χειρισμό κινδύνων και περιστατικών σύμφωνα με το άρθρο 10 της οδηγίας (ΕΕ) 2022/2555·

4) «περιουσιακό στοιχείο κρίσιμου αντικτύπου»: περιουσιακό στοιχείο που είναι απαραίτητο για την εκτέλεση διαδικασίας κρίσιμου αντικτύπου·

5) «οντότητα κρίσιμου αντικτύπου»: οντότητα που εκτελεί διαδικασία κρίσιμου αντικτύπου και προσδιορίζεται από τις αρμόδιες αρχές σύμφωνα με το άρθρο 24·

6) «περίμετρος κρίσιμου αντικτύπου»: περίμετρος που ορίζεται από οντότητα αναφερόμενη στο άρθρο 2 παράγραφος 1, που περικλείει όλα τα περιουσιακά στοιχεία κρίσιμου αντικτύπου και στην οποία μπορεί να ελεγχθεί η πρόσβαση στα εν λόγω περιουσιακά στοιχεία και η οποία καθορίζει το πεδίο όπου εφαρμόζονται οι προηγμένοι έλεγχοι κυβερνοασφάλειας·

7) «διαδικασία κρίσιμου αντικτύπου»: επιχειρηματική διαδικασία που εκτελείται από οντότητα για την οποία οι δείκτες αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας υπερβαίνουν το όριο κρίσιμου αντικτύπου·

8) «όριο κρίσιμου αντικτύπου»: οι τιμές των δεικτών αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας που αναφέρονται στο άρθρο 19 παράγραφος 3 στοιχείο β), πάνω από τις οποίες μια κυβερνοεπίθεση σε επιχειρηματική διαδικασία θα προκαλέσει κρίσιμη διατάραξη των διασυνοριακών ροών ηλεκτρικής ενέργειας·

9) «πάροχος κρίσιμων υπηρεσιών ΤΠΕ»: οντότητα η οποία παρέχει υπηρεσία ΤΠΕ ή διαδικασία ΤΠΕ που είναι απαραίτητη για διαδικασία κρίσιμου ή υψηλού αντικτύπου η οποία επηρεάζει πτυχές κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας και η οποία, εάν τεθεί σε κίνδυνο, μπορεί να προκαλέσει κυβερνοεπίθεση με αντίκτυπο που υπερβαίνει το όριο κρίσιμου ή υψηλού αντικτύπου·

10) «διασυνοριακή ροή ηλεκτρικής ενέργειας»: διασυνοριακή ροή όπως ορίζεται στο άρθρο 2 σημείο 3) του κανονισμού (ΕΕ) 2019/943·

11) «κυβερνοεπίθεση»: περιστατικό όπως ορίζεται στο άρθρο 3 σημείο 14) του κανονισμού (ΕΕ) 2022/2554·

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

13) «έλεγχος κυβερνοασφάλειας»: οι ενέργειες ή οι διαδικασίες που εκτελούνται με σκοπό την αποφυγή, την ανίχνευση, την αντιμετώπιση ή την ελαχιστοποίηση των κινδύνων για την κυβερνοασφάλεια·

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

15) «σύστημα διαχείρισης της κυβερνοασφάλειας»: οι πολιτικές, οι διαδικασίες, οι κατευθυντήριες γραμμές και οι συναφείς πόροι και δραστηριότητες, που τελούν υπό τη συλλογική διαχείριση οντότητας, με σκοπό την προστασία των πληροφοριακών πόρων της από κυβερνοαπειλές, και οι οποίες συστηματικά θεσπίζουν, υλοποιούν, διαχειρίζονται, παρακολουθούν, επανεξετάζουν, διατηρούν και βελτιώνουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών ενός οργανισμού·

16) «κέντρο επιχειρήσεων κυβερνοασφάλειας»: ειδικό κέντρο στο οποίο τεχνική ομάδα αποτελούμενη από έναν ή περισσότερους εμπειρογνώμονες, υποστηριζόμενους από συστήματα ΤΠ για την κυβερνοασφάλεια, εκτελεί καθήκοντα σχετικά με την ασφάλεια [υπηρεσίες κέντρου επιχειρήσεων κυβερνοασφάλειας (CSOC)], όπως χειρισμό κυβερνοεπιθέσεων και σφαλμάτων στη διαμόρφωση της ασφάλειας, παρακολούθηση της ασφάλειας, ανάλυση αρχείων καταγραφής και ανίχνευση κυβερνοεπιθέσεων·

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

18) «διαχείριση ευπαθειών στον τομέα της κυβερνοασφάλειας»: πρακτική εντοπισμού και αντιμετώπισης ευπαθειών·

19) «οντότητα»: οντότητα όπως ορίζεται στο άρθρο 6 σημείο 38) της οδηγίας (ΕΕ) 2022/2555·

20) «έγκαιρη προειδοποίηση»: οι πληροφορίες που απαιτούνται για να δηλωθεί αν υπάρχουν υπόνοιες ότι το σημαντικό περιστατικό έχει προκληθεί από παράνομες ή κακόβουλες πράξεις ή θα μπορούσε να έχει διασυνοριακές επιπτώσεις·

21) «δείκτης αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας» ή «ECII»: δείκτης ή κλίμακα ταξινόμησης που κατατάσσει τις πιθανές συνέπειες κυβερνοεπιθέσεων σε επιχειρηματικές διαδικασίες που εμπλέκονται σε διασυνοριακές ροές ηλεκτρικής ενέργειας·

22) «ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας»: σχήμα όπως ορίζεται στο άρθρο 2 σημείο 9) του κανονισμού (ΕΕ) 2019/881·

23) «οντότητα υψηλού αντικτύπου»: οντότητα που εκτελεί διαδικασία υψηλού αντικτύπου και προσδιορίζεται από τις αρμόδιες αρχές σύμφωνα με το άρθρο 24·

24) «διαδικασία υψηλού αντικτύπου»: οποιαδήποτε επιχειρηματική διαδικασία που εκτελείται από οντότητα για την οποία οι δείκτες αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας υπερβαίνουν το όριο υψηλού αντικτύπου·

25) «περιουσιακό στοιχείο υψηλού αντικτύπου»: περιουσιακό στοιχείο που είναι απαραίτητο για την εκτέλεση διαδικασίας υψηλού αντικτύπου·

26) «όριο υψηλού αντικτύπου»: οι τιμές των δεικτών αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας που αναφέρονται στο άρθρο 19 παράγραφος 3 στοιχείο β), πάνω από τις οποίες μια επιτυχημένη κυβερνοεπίθεση σε διαδικασία θα προκαλέσει μεγάλη διαταραχή των διασυνοριακών ροών ηλεκτρικής ενέργειας·

27) «περίμετρος υψηλού αντικτύπου»: περίμετρος που ορίζεται από οποιαδήποτε οντότητα αναφερόμενη στο άρθρο 2 παράγραφος 1, η οποία περικλείει όλα τα περιουσιακά στοιχεία υψηλού αντικτύπου, στην οποία μπορεί να ελεγχθεί η πρόσβαση στα εν λόγω περιουσιακά στοιχεία και η οποία καθορίζει το πεδίο όπου εφαρμόζονται οι ελάχιστοι έλεγχοι κυβερνοασφάλειας·

28) «προϊόν ΤΠΕ»: προϊόν ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 12) του κανονισμού (ΕΕ) 2019/881·

29) «υπηρεσία ΤΠΕ»: υπηρεσία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 13) του κανονισμού (ΕΕ) 2019/881·

30) «διαδικασία ΤΠΕ»: διαδικασία ΤΠΕ όπως ορίζεται στο άρθρο 2 σημείο 14) του κανονισμού (ΕΕ) 2019/881·

31) «παρωχημένο σύστημα»: παρωχημένο σύστημα ΤΠΕ όπως ορίζεται στο άρθρο 3 σημείο 3) του κανονισμού (ΕΕ) 2022/2554·

32) «εθνικό ενιαίο σημείο επαφής»: το ενιαίο σημείο επαφής που ορίζεται ή συστήνεται από κάθε κράτος μέλος σύμφωνα με το άρθρο 8 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555·

33) «αρχές διαχείρισης κυβερνοκρίσεων NIS»: οι αρχές που ορίζονται ή συστήνονται σύμφωνα με το άρθρο 9 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555·

34) «φορέας προέλευσης»: οντότητα που ξεκινά γεγονός ανταλλαγής πληροφοριών, κοινοποίησης πληροφοριών ή αποθήκευσης πληροφοριών·

35) «προδιαγραφές δημόσιων συμβάσεων»: οι προδιαγραφές που καθορίζουν οι οντότητες για τις δημόσιες συμβάσεις νέων ή επικαιροποιημένων προϊόντων ΤΠΕ, διαδικασιών ΤΠΕ ή υπηρεσιών ΤΠΕ·

36) «εκπρόσωπος»: φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ένωση το οποίο έχει οριστεί ρητά να ενεργεί εξ ονόματος οντότητας υψηλού ή κρίσιμου αντικτύπου που δεν είναι εγκατεστημένη στην Ένωση αλλά παρέχει υπηρεσίες σε οντότητες εντός της Ένωσης και στο οποίο μπορεί να απευθύνεται αρμόδια αρχή ή CSIRT αντί της ίδιας της οντότητας υψηλού ή κρίσιμου αντικτύπου όσον αφορά τις υποχρεώσεις της εν λόγω οντότητας δυνάμει του παρόντος κανονισμού·

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

38) «πίνακας αντικτύπου κινδύνων»: πίνακας που χρησιμοποιείται κατά την εκτίμηση κινδύνων για τον προσδιορισμό του επιπέδου αντικτύπου κινδύνου που προκύπτει για κάθε κίνδυνο που αξιολογείται·

39) «ταυτόχρονη κρίση ηλεκτρικής ενέργειας»: κρίση ηλεκτρικής ενέργειας όπως ορίζεται στο άρθρο 2 σημείο 10) του κανονισμού (ΕΕ) 2019/941·

40) «ενιαίο σημείο επαφής σε επίπεδο οντότητας»: ενιαίο σημείο επαφής σε επίπεδο οντότητας όπως ορίζεται στο άρθρο 38 παράγραφος 1 στοιχείο γ)·

41) «ενδιαφερόμενο μέρος»: κάθε μέρος που έχει συμφέρον στην επιτυχία και στη συνεχή λειτουργία μιας οργάνωσης ή διαδικασίας, όπως οι υπάλληλοι, τα διοικητικά στελέχη, οι μέτοχοι, οι ρυθμιστικές αρχές, οι ενώσεις, οι προμηθευτές και οι πελάτες·

42) «πρότυπο»: πρότυπο όπως ορίζεται στο άρθρο 2 σημείο 1) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([16])·

43) «λειτουργική περιφέρεια συστήματος»: οι λειτουργικές περιφέρειες συστήματος όπως ορίζονται στο παράρτημα I της απόφασης 05-2022 του ACER για τον ορισμό των λειτουργικών περιφερειών συστήματος, οι οποίες συστήνονται σύμφωνα με το άρθρο 36 του κανονισμού (ΕΕ) 2019/943·

44) «διαχειριστές συστημάτων»: «διαχειριστής συστήματος διανομής» (στο εξής: ΔΣΔ) και «διαχειριστής συστήματος μεταφοράς» (στο εξής: ΔΣΜ), όπως ορίζονται στο άρθρο 2 σημεία 29) και 35) της οδηγίας (ΕΕ) 2019/944·

45) «διαδικασία κρίσιμου αντικτύπου σε επίπεδο Ένωσης»: κάθε διαδικασία στον τομέα της ηλεκτρικής ενέργειας, στην οποία ενδέχεται να συμμετέχουν πολλές οντότητες, για την οποία ο πιθανός αντίκτυπος μιας κυβερνοεπίθεσης μπορεί να θεωρηθεί κρίσιμος κατά τη διενέργεια της εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης·

46) «διαδικασία υψηλού αντικτύπου σε επίπεδο Ένωσης»: κάθε διαδικασία στον τομέα της ηλεκτρικής ενέργειας, στην οποία ενδέχεται να συμμετέχουν πολλές οντότητες, για την οποία ο πιθανός αντίκτυπος μιας κυβερνοεπίθεσης μπορεί να θεωρηθεί υψηλός κατά τη διενέργεια της εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης·

47) «μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης»: ευπάθεια η οποία δεν έχει ακόμη δημοσιοποιηθεί και διορθωθεί και για την οποία υπάρχουν αξιόπιστα στοιχεία που αποδεικνύουν ότι πραγματοποιήθηκε εκτέλεση κακόβουλου κώδικα από παράγοντα σε σύστημα χωρίς την άδεια του ιδιοκτήτη του συστήματος·

48) «ευπάθεια»: ευπάθεια όπως ορίζεται στο άρθρο 6 σημείο 15) της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 4

Αρμόδια αρχή

1. Το συντομότερο δυνατόν και σε κάθε περίπτωση έως τις 13ης Δεκεμβρίου 2024, κάθε κράτος μέλος ορίζει εθνική κυβερνητική ή ρυθμιστική αρχή υπεύθυνη για την εκτέλεση των καθηκόντων που της ανατίθενται με τον παρόντα κανονισμό (στο εξής: αρμόδια αρχή). Έως ότου ανατεθεί στην αρμόδια αρχή η εκτέλεση των καθηκόντων δυνάμει του παρόντος κανονισμού, η ρυθμιστική αρχή που ορίζεται από κάθε κράτος μέλος σύμφωνα με το άρθρο 57 παράγραφος 1 της οδηγίας (ΕΕ) 2019/944 εκτελεί τα καθήκοντα της αρμόδιας αρχής σύμφωνα με τον παρόντα κανονισμό.

2. Τα κράτη μέλη ειδοποιούν, χωρίς καθυστέρηση, την Επιτροπή, τον ACER, τον ENISA, την Ομάδα Συνεργασίας NIS που έχει συσταθεί σύμφωνα με το άρθρο 14 της οδηγίας (ΕΕ) 2022/2555 και τη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού που έχει συσταθεί δυνάμει του άρθρου 1 της απόφασης της Επιτροπής, της 15ης Νοεμβρίου 2012 ([17]), και τους κοινοποιούν το όνομα και τα στοιχεία επικοινωνίας της οικείας αρμόδιας αρχής που ορίζεται σύμφωνα με την παράγραφο 1 του παρόντος άρθρου και τυχόν μεταγενέστερες αλλαγές σε αυτά.

([16]) Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012 , σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).

([17]) Απόφαση της Επιτροπής, της 15ης Νοεμβρίου 2012, για τη σύσταση της Συντονιστικής Ομάδας στον τομέα του Ηλεκτρισμού (2012/C 353/02) (ΕΕ C 353 της 17.11.2012, σ. 2)

3. Τα κράτη μέλη μπορούν να επιτρέπουν στην οικεία αρμόδια αρχή να αναθέτει καθήκοντα που της ανατίθενται με τον παρόντα κανονισμό σε άλλες εθνικές αρχές, με εξαίρεση τα καθήκοντα που αναφέρονται στο άρθρο 5. Κάθε αρμόδια αρχή παρακολουθεί την εφαρμογή του παρόντος κανονισμού από τις αρχές στις οποίες έχει αναθέσει καθήκοντα. Η αρμόδια αρχή κοινοποιεί το όνομα και τα στοιχεία επικοινωνίας των αρχών στις οποίες έχει αναθέσει καθήκοντα, τα καθήκοντα που έχουν ανατεθεί και τυχόν μεταγενέστερες αλλαγές στα στοιχεία αυτά στην Επιτροπή, στον ACER, στη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού, στον ENISA και στην Ομάδα Συνεργασίας NIS.

Άρθρο 5

Συνεργασία μεταξύ των αρμόδιων αρχών και φορέων σε εθνικό επίπεδο

Οι αρμόδιες αρχές συντονίζουν και διασφαλίζουν την κατάλληλη συνεργασία μεταξύ των αρμόδιων αρχών που είναι υπεύθυνες για την κυβερνοασφάλεια, των αρχών διαχείρισης κυβερνοκρίσεων, των εθνικών ρυθμιστικών αρχών, των αρμόδιων αρχών για την ετοιμότητα αντιμετώπισης κινδύνων και των CSIRT για τους σκοπούς της εκπλήρωσης των σχετικών υποχρεώσεων που ορίζονται στον παρόντα κανονισμό. Οι αρμόδιες αρχές συντονίζονται επίσης με άλλους φορείς ή αρχές που καθορίζονται από κάθε κράτος μέλος, ώστε να διασφαλίζονται αποδοτικές διαδικασίες και να αποφεύγονται οι αλληλεπικαλύψεις καθηκόντων και υποχρεώσεων. Οι αρμόδιες αρχές μπορούν να δώσουν εντολή στις αντίστοιχες εθνικές ρυθμιστικές αρχές να ζητήσουν γνωμοδότηση από τον ACER σύμφωνα με το άρθρο 8 παράγραφος 3.

Άρθρο 6

Όροι και προϋποθέσεις ή μεθοδολογίες ή σχέδια

1. Οι ΔΣΜ καταρτίζουν, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, προτάσεις για τους όρους και τις προϋποθέσεις ή τις μεθοδολογίες σύμφωνα με την παράγραφο 2, ή για σχέδια σύμφωνα με την παράγραφο 3.

2. Οι παρακάτω όροι και προϋποθέσεις ή μεθοδολογίες και τυχόν τροποποιήσεις αυτών υπόκεινται σε έγκριση από όλες τις αρμόδιες αρχές:

α) οι μεθοδολογίες εκτίμησης κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 18 παράγραφος 1·

β) η συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας σύμφωνα με το άρθρο 23·

γ) οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας σύμφωνα με το άρθρο 29, η χαρτογράφηση των ελέγχων κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας με βάση τα πρότυπα που ορίζονται στο άρθρο 34, συμπεριλαμβανομένων ελάχιστων και προηγμένων ελέγχων κυβερνοασφάλειας στην αλυσίδα εφοδιασμού σύμφωνα με το άρθρο 33·

δ) σύσταση για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 35·

ε) η μεθοδολογία της κλίμακας ταξινόμησης κυβερνοεπιθέσεων σύμφωνα με το άρθρο 37 παράγραφος 8.

3. Οι προτάσεις για τα περιφερειακά σχέδια μετριασμού των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 22 υπόκεινται σε έγκριση από όλες τις αρμόδιες αρχές της οικείας λειτουργικής περιφέρειας συστήματος.

4. Οι προτάσεις για όρους και προϋποθέσεις ή μεθοδολογίες που αναφέρονται στην παράγραφο 2 ή για σχέδια που αναφέρονται στην παράγραφο 3 περιλαμβάνουν προτεινόμενο χρονοδιάγραμμα για την εφαρμογή τους και περιγραφή του αναμενόμενου αντικτύπου τους στους στόχους του παρόντος κανονισμού.

5. Ο φορέας ΔΣΔ της ΕΕ μπορεί να υποβάλει αιτιολογημένη γνώμη στους ενδιαφερόμενους ΔΣΜ έως 3 εβδομάδες πριν από τη λήξη της προθεσμίας υποβολής της πρότασης όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, στις αρμόδιες αρχές. Οι ΔΣΜ που είναι υπεύθυνοι για την πρόταση όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, λαμβάνουν υπόψη την αιτιολογημένη γνώμη του φορέα ΔΣΔ της ΕΕ πριν από την υποβολή της πρότασης στις αρμόδιες αρχές προς έγκριση. Οι ΔΣΜ αιτιολογούν τις περιπτώσεις στις οποίες δεν λαμβάνεται υπόψη η γνώμη του φορέα ΔΣΔ της ΕΕ.

6. Κατά την από κοινού κατάρτιση όρων, προϋποθέσεων, μεθοδολογιών και σχεδίων, οι συμμετέχοντες ΔΣΜ συνεργάζονται στενά. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, ενημερώνουν τακτικά τις αρμόδιες αρχές και τον ACER σχετικά με την πρόοδο ως προς την κατάρτιση των όρων και προϋποθέσεων ή μεθοδολογιών, ή των σχεδίων.

Άρθρο 7

Κανόνες ψηφοφορίας στους ΔΣΜ

1. Όταν οι ΔΣΜ που αποφασίζουν επί προτάσεων όρων και προϋποθέσεων ή μεθοδολογιών δεν μπορούν να καταλήξουν σε συμφωνία, αποφασίζουν με ειδική πλειοψηφία. Η ειδική πλειοψηφία για τις εν λόγω προτάσεις υπολογίζεται ως εξής:

α) ΔΣΜ που εκπροσωπούν τουλάχιστον το 55 % των κρατών μελών· και

β) ΔΣΜ που εκπροσωπούν κράτη μέλη τα οποία συγκεντρώνουν τουλάχιστον το 65 % του πληθυσμού της Ένωσης.

2. Η μειοψηφία αρνησικυρίας για αποφάσεις επί προτάσεων για όρους και προϋποθέσεις ή μεθοδολογίες που αναφέρονται στο άρθρο 6 παράγραφος 2 αποτελείται από ΔΣΜ που εκπροσωπούν τουλάχιστον τέσσερα κράτη μέλη, ειδάλλως θεωρείται ότι επιτυγχάνεται ειδική πλειοψηφία.

3. Όταν οι ΔΣΜ μιας λειτουργικής περιοχής συστήματος που αποφασίζουν επί προτάσεων για σχέδια που αναφέρονται στο άρθρο 6 παράγραφος 2 δεν μπορούν να καταλήξουν σε συμφωνία και όταν η οικεία λειτουργική περιοχή συστήματος αποτελείται από περισσότερα από πέντε κράτη μέλη, οι ΔΣΜ αποφασίζουν με ειδική πλειοψηφία. Η ειδική πλειοψηφία για προτάσεις που αναφέρονται στο άρθρο 6 παράγραφος 2 συνίσταται στην εξής πλειοψηφία:

α) των ΔΣΜ που εκπροσωπούν τουλάχιστον το 72 % των οικείων κρατών μελών· και

β) των ΔΣΜ που εκπροσωπούν κράτη μέλη τα οποία συγκεντρώνουν τουλάχιστον το 65 % του πληθυσμού της συγκεκριμένης περιοχής.

4. Η μειοψηφία αρνησικυρίας για αποφάσεις επί προτάσεων για σχέδια περιλαμβάνει τουλάχιστον τον ελάχιστο αριθμό των ΔΣΜ που εκπροσωπούν πάνω από το 35 % του πληθυσμού των συμμετεχόντων κρατών μελών, συν τους ΔΣΜ που εκπροσωπούν τουλάχιστον ένα επιπλέον οικείο κράτος μέλος, ειδάλλως θεωρείται ότι επιτυγχάνεται ειδική πλειοψηφία.

5. Για τις αποφάσεις των ΔΣΜ επί προτάσεων όρων και προϋποθέσεων ή μεθοδολογιών σύμφωνα με το άρθρο 6 παράγραφος 2, αποδίδεται μία ψήφος ανά κράτος μέλος. Εάν υπάρχουν περισσότεροι του ενός ΔΣΜ στην επικράτεια κράτους μέλους, το κράτος μέλος κατανέμει τα δικαιώματα ψήφου μεταξύ των ΔΣΜ.

6. Εάν οι ΔΣΜ, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, δεν υποβάλουν αρχική ή τροποποιημένη πρόταση όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, στις σχετικές αρμόδιες αρχές εντός των προθεσμιών που ορίζονται στον παρόντα κανονισμό, υποβάλλουν στις σχετικές αρμόδιες αρχές και στον ACER τα σχετικά σχέδια όρων και προϋποθέσεων ή μεθοδολογιών ή τα σχετικά προσχέδια. Εξηγούν τους λόγους που τους εμπόδισαν να καταλήξουν σε συμφωνία. Οι αρμόδιες αρχές λαμβάνουν από κοινού τα κατάλληλα μέτρα για την έγκριση των απαιτούμενων όρων και προϋποθέσεων ή μεθοδολογιών, ή των απαιτούμενων σχεδίων. Αυτό μπορούν να το πράξουν για παράδειγμα, ζητώντας τροποποιήσεις στα προσχέδια σύμφωνα με την παρούσα παράγραφο, αναθεωρώντας και συμπληρώνοντας τα εν λόγω προσχέδια ή, εάν δεν έχουν υποβληθεί προσχέδια, καθορίζοντας και εγκρίνοντας τους απαιτούμενους όρους και προϋποθέσεις ή μεθοδολογίες ή τα απαιτούμενα σχέδια.

Άρθρο 8

Υποβολή προτάσεων στις αρμόδιες αρχές

1. Οι ΔΣΜ υποβάλλουν τις προτάσεις για όρους και προϋποθέσεις ή μεθοδολογίες ή για σχέδια προς έγκριση στις σχετικές αρμόδιες αρχές εντός των αντίστοιχων προθεσμιών που ορίζονται στα άρθρα 18, 23, 29, 33, 34, 35 και 37. Οι αρμόδιες αρχές μπορούν να παρατείνουν από κοινού τις εν λόγω προθεσμίες σε εξαιρετικές περιστάσεις, κυρίως σε περιπτώσεις στις οποίες η προθεσμία δεν μπορεί να τηρηθεί λόγω περιστάσεων εκτός της σφαίρας επιρροής των ΔΣΜ ή του φορέα ΔΣΔ της ΕΕ.

2. Οι προτάσεις για όρους και προϋποθέσεις ή μεθοδολογίες ή για σχέδια σύμφωνα με την παράγραφο 1 υποβάλλονται προς ενημέρωση στον ACER ταυτόχρονα με την υποβολή τους στις αρμόδιες αρχές.

3. Κατόπιν κοινού αιτήματος των εθνικών ρυθμιστικών αρχών, ο ACER εκδίδει γνωμοδότηση σχετικά με την πρόταση για όρους και προϋποθέσεις ή μεθοδολογίες ή για σχέδια, εντός έξι μηνών από την παραλαβή των προτάσεων για όρους και προϋποθέσεις ή μεθοδολογίες ή για σχέδια, και κοινοποιεί τη γνώμη στις εθνικές ρυθμιστικές αρχές και τις αρμόδιες αρχές. Οι εθνικές ρυθμιστικές αρχές, οι ΕΑΑ κυβερνοασφάλειας και οποιεσδήποτε άλλες αρχές που ορίζονται ως αρμόδιες αρχές συντονίζονται μεταξύ τους προτού οι εθνικές ρυθμιστικές αρχές ζητήσουν τη γνωμοδότηση του ACER. Ο ACER μπορεί να συμπεριλάβει συστάσεις στην εν λόγω γνωμοδότηση. Ο ACER ζητεί τη γνώμη του ENISA προτού εκδώσει γνωμοδότηση επί των προτάσεων που αναφέρονται στο άρθρο 6 παράγραφος 2.

4. Οι αρμόδιες αρχές διαβουλεύονται, συνεργάζονται στενά και συντονίζονται μεταξύ τους προκειμένου να καταλήξουν σε συμφωνία σχετικά με τους προτεινόμενους όρους και προϋποθέσεις, μεθοδολογίες ή σχέδια. Πριν από την έγκριση των όρων και προϋποθέσεων ή μεθοδολογιών, ή των σχεδίων, αναθεωρούν και συμπληρώνουν τις προτάσεις, κατά περίπτωση, αφού ζητήσουν τη γνώμη του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ, προκειμένου να διασφαλιστεί ότι οι προτάσεις συνάδουν με τον παρόντα κανονισμό και συμβάλλουν στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση.

5. Οι αρμόδιες αρχές αποφασίζουν επί των όρων και προϋποθέσεων ή μεθοδολογιών ή επί των σχεδίων εντός έξι μηνών από την παραλαβή των όρων και προϋποθέσεων ή μεθοδολογιών ή των σχεδίων από τη σχετική αρμόδια αρχή ή, κατά περίπτωση, από την τελευταία σχετική ενδιαφερόμενη αρμόδια αρχή.

6. Όταν ο ACER εκδίδει γνωμοδότηση, οι σχετικές αρμόδιες αρχές λαμβάνουν υπόψη την εν λόγω γνωμοδότηση και λαμβάνουν τις αποφάσεις τους εντός έξι μηνών από την παραλαβή της γνωμοδότησης του ACER.

7. Όταν οι αρμόδιες αρχές απαιτούν από κοινού τροποποίηση των προτεινόμενων όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, προκειμένου να τα εγκρίνουν, οι ΔΣΜ καταρτίζουν, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, πρόταση για την εν λόγω τροποποίηση των όρων και προϋποθέσεων ή μεθοδολογιών ή των σχεδίων. Οι ΔΣΜ υποβάλλουν την τροποποιημένη πρόταση προς έγκριση εντός δύο μηνών από το αίτημα των αρμόδιων αρχών. Οι αρμόδιες αρχές λαμβάνουν απόφαση επί των τροποποιημένων όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, εντός δύο μηνών από την υποβολή τους.

8. Εάν οι αρμόδιες αρχές δεν καταφέρουν να καταλήξουν σε συμφωνία εντός της προθεσμίας που αναφέρεται στην παράγραφο 5 ή 7, ενημερώνουν σχετικά την Επιτροπή. Η Επιτροπή μπορεί να λάβει κατάλληλα μέτρα για να καταστήσει δυνατή την έγκριση των απαιτούμενων όρων και προϋποθέσεων ή μεθοδολογιών ή των απαιτούμενων σχεδίων.

9. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, και ο φορέας ΔΣΔ της ΕΕ δημοσιεύουν τους όρους και προϋποθέσεις ή τις μεθοδολογίες, ή τα σχέδια. στους δικτυακούς τόπους τους κατόπιν έγκρισης από τις σχετικές αρμόδιες αρχές, εκτός εάν οι εν λόγω πληροφορίες θεωρούνται εμπιστευτικές σύμφωνα με το άρθρο 47.

10. Οι αρμόδιες αρχές μπορούν να ζητήσουν από κοινού προτάσεις τροποποίησης των εγκεκριμένων όρων και προϋποθέσεων ή μεθοδολογιών, ή των εγκεκριμένων σχεδίων, από τους ΔΣΜ και τον φορέα ΔΣΔ της ΕΕ και να καθορίσουν προθεσμία για την υποβολή των εν λόγω προτάσεων. Οι ΔΣΜ, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, μπορούν επίσης να προτείνουν τροποποιήσεις στις αρμόδιες αρχές με δική τους πρωτοβουλία. Οι προτάσεις τροποποίησης των όρων και προϋποθέσεων ή μεθοδολογιών, ή τροποποίησης των σχεδίων, καταρτίζονται και εγκρίνονται σύμφωνα με τη διαδικασία του παρόντος άρθρου.

11. Τουλάχιστον ανά τριετία μετά την πρώτη έγκριση των αντίστοιχων όρων και προϋποθέσεων ή μεθοδολογιών, ή των αντίστοιχων εγκεκριμένων σχεδίων, οι ΔΣΜ, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, επανεξετάζουν την αποτελεσματικότητα των εγκεκριμένων όρων και προϋποθέσεων ή μεθοδολογιών, ή των εγκεκριμένων σχεδίων, και αναφέρουν τα πορίσματα της επανεξέτασης στις αρμόδιες αρχές και στον ACER χωρίς αδικαιολόγητη καθυστέρηση.

Άρθρο 9

Διαβούλευση

1. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, διαβουλεύονται με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων του ACER, του ENISA και της αρμόδιας αρχής κάθε κράτους μέλους, σχετικά με τα σχέδια προτάσεων όρων και προϋποθέσεων ή μεθοδολογιών που αναφέρονται στο άρθρο 6 παράγραφος 2 και σχεδίων που αναφέρονται στο άρθρο 6 παράγραφος 3. Η διαβούλευση διαρκεί για τουλάχιστον έναν μήνα.

2. Οι προτάσεις όρων και προϋποθέσεων ή μεθοδολογιών που αναφέρονται στο άρθρο 6 παράγραφος 2, οι οποίες υποβάλλονται από τους ΔΣΜ, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, δημοσιεύονται και υποβάλλονται προς διαβούλευση σε επίπεδο Ένωσης. Οι προτάσεις σχεδίων που αναφέρονται στο άρθρο 6 παράγραφος 3, οι οποίες υποβάλλονται από τους οικείους ΔΣΜ, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, σε περιφερειακό επίπεδο υποβάλλονται προς διαβούλευση τουλάχιστον σε περιφερειακό επίπεδο.

3. Οι ΔΣΜ, με τη βοήθεια του ΕΔΔΣΜ ηλεκτρικής ενέργειας, και ο φορέας ΔΣΔ της ΕΕ που είναι αρμόδιοι για την υποβολή προτάσεων όρων και προϋποθέσεων ή μεθοδολογιών, ή σχεδίων, λαμβάνουν δεόντως υπόψη τις απόψεις των ενδιαφερόμενων μερών που διατυπώνονται κατά τις διαβουλεύσεις που διενεργούνται σύμφωνα με την παράγραφο 1, πριν από την υποβολή της πρότασης για έγκριση από τις ρυθμιστικές αρχές. Σε κάθε περίπτωση, κατά την υποβολή παρέχεται τεκμηριωμένη αιτιολόγηση της αποδοχής ή μη αποδοχής των απόψεων που διατυπώθηκαν κατά τη διαβούλευση, η οποία δημοσιεύεται εγκαίρως, πριν από την πρόταση όρων και προϋποθέσεων ή μεθοδολογιών ή ταυτόχρονα με αυτήν.

Άρθρο 10

Συμμετοχή των ενδιαφερόμενων μερών

Ο ACER, σε στενή συνεργασία με το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, οργανώνει τη συμμετοχή των ενδιαφερόμενων μερών, συμπεριλαμβανομένων τακτικών συναντήσεων με τα ενδιαφερόμενα μέρη για τον εντοπισμό προβλημάτων και τη διατύπωση προτάσεων για βελτιώσεις που σχετίζονται με την εφαρμογή του παρόντος κανονισμού.

Άρθρο 11

Ανάκτηση των δαπανών

1. Οι δαπάνες οι οποίες βαρύνουν τους ΔΣΜ και τους ΔΣΔ που υπόκεινται σε ρύθμιση τιμολογίων δικτύου και απορρέουν από τις υποχρεώσεις που ορίζονται στον παρόντα κανονισμό, συμπεριλαμβανομένων των δαπανών οι οποίες βαρύνουν το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, αξιολογούνται από τη σχετική εθνική ρυθμιστική αρχή κάθε κράτους μέλους.

2. Οι δαπάνες που αξιολογούνται ως εύλογες, αποδοτικές και αναλογικές ανακτώνται μέσω τιμολογίων δικτύου ή άλλων κατάλληλων μηχανισμών, όπως καθορίζονται από τη σχετική εθνική ρυθμιστική αρχή.

3. Εάν ζητηθεί από τις σχετικές εθνικές ρυθμιστικές αρχές, οι ΔΣΜ και οι ΔΣΔ που αναφέρονται στην παράγραφο 1 παρέχουν, εντός εύλογου χρονικού διαστήματος που καθορίζεται από την εθνική ρυθμιστική αρχή, τις πληροφορίες που είναι αναγκαίες για τη διευκόλυνση της αξιολόγησης των δαπανών που προκύπτουν.

Άρθρο 12

Παρακολούθηση

1. Ο ACER παρακολουθεί την εφαρμογή του παρόντος κανονισμού σύμφωνα με το άρθρο 32 παράγραφος 1 του κανονισμού (ΕΕ) 2019/943 και το άρθρο 4 παράγραφος 2 του κανονισμού (ΕΕ) 2019/942. Κατά τη διενέργεια της εν λόγω παρακολούθησης, ο ACER μπορεί να συνεργάζεται με τον ENISA και να ζητεί υποστήριξη από το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ. Ο ACER ενημερώνει τακτικά τη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού και την Ομάδα Συνεργασίας NIS σχετικά με την εφαρμογή του παρόντος κανονισμού.

2. Ο ACER δημοσιεύει έκθεση τουλάχιστον ανά τριετία μετά την έναρξη ισχύος του παρόντος κανονισμού για:

α) την επανεξέταση της κατάστασης υλοποίησης των εφαρμοστέων μέτρων διαχείρισης κινδύνων για την κυβερνοασφάλεια όσον αφορά τις οντότητες υψηλού αντικτύπου και τις οντότητες κρίσιμου αντικτύπου·

β) τον προσδιορισμό του αν ενδέχεται να απαιτούνται πρόσθετοι κανόνες σχετικά με τις κοινές απαιτήσεις, τον προγραμματισμό, την παρακολούθηση, την υποβολή εκθέσεων και τη διαχείριση κρίσεων με στόχο την πρόληψη κινδύνων για τον τομέα της ηλεκτρικής ενέργειας· και

γ) τον προσδιορισμό τομέων βελτίωσης για την αναθεώρηση του παρόντος κανονισμού ή τον καθορισμό τομέων που δεν καλύπτονται και νέων προτεραιοτήτων που ενδέχεται να προκύψουν λόγω τεχνολογικών εξελίξεων.

3. Έως τις 13 Ιουνίου 2025 ο ACER, σε συνεργασία με τον ENISA και κατόπιν διαβούλευσης με το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, μπορεί να εκδίδει καθοδήγηση για τις σχετικές πληροφορίες που πρέπει να κοινοποιούνται στον ACER για σκοπούς παρακολούθησης, καθώς και για τη διαδικασία και τη συχνότητα της συλλογής, με βάση τους δείκτες επιδόσεων που ορίζονται σύμφωνα με την παράγραφο 5.

4. Οι αρμόδιες αρχές μπορούν να έχουν πρόσβαση στις σχετικές πληροφορίες που έχει στην κατοχή του ο ACER και τις οποίες έχει συλλέξει σύμφωνα με το παρόν άρθρο.

5. Ο ACER, σε συνεργασία με τον ENISA και με την υποστήριξη του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ, εκδίδει μη δεσμευτικούς δείκτες επιδόσεων για την αξιολόγηση της επιχειρησιακής αξιοπιστίας που σχετίζονται με πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας.

6. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 του παρόντος κανονισμού υποβάλλουν στον ACER τις πληροφορίες που απαιτούνται για την εκτέλεση των καθηκόντων του ACER που αναφέρονται στην παράγραφο 2.

Άρθρο 13

Συγκριτική αξιολόγηση

1. Έως τις 13 Ιουνίου 2025 ο ACER, σε συνεργασία με τον ENISA, καταρτίζει μη δεσμευτικό οδηγό συγκριτικής αξιολόγησης της κυβερνοασφάλειας. Ο οδηγός εξηγεί στις εθνικές ρυθμιστικές αρχές τις αρχές συγκριτικής αξιολόγησης των εφαρμοζόμενων ελέγχων κυβερνοασφάλειας σύμφωνα με την παράγραφο 2 του παρόντος άρθρου, λαμβάνοντας υπόψη το κόστος υλοποίησης των ελέγχων και την αποτελεσματικότητα της λειτουργίας που επιτελούν οι διαδικασίες, τα προϊόντα, οι υπηρεσίες, τα συστήματα και οι λύσεις που χρησιμοποιούνται για την υλοποίηση των εν λόγω ελέγχων. Ο ACER λαμβάνει υπόψη τις υπάρχουσες εκθέσεις συγκριτικής αξιολόγησης κατά την κατάρτιση του μη δεσμευτικού οδηγού συγκριτικής αξιολόγησης της κυβερνοασφάλειας. Ο ACER υποβάλλει προς ενημέρωση στις εθνικές ρυθμιστικές αρχές τον μη δεσμευτικό οδηγό συγκριτικής αξιολόγησης της κυβερνοασφάλειας.

2. Εντός 12 μηνών από την κατάρτιση του οδηγού συγκριτικής αξιολόγησης σύμφωνα με την παράγραφο 1, οι εθνικές ρυθμιστικές αρχές διενεργούν ανάλυση συγκριτικής αξιολόγησης για να αξιολογήσουν αν οι τρέχουσες επενδύσεις στην κυβερνοασφάλεια:

α) μετριάζουν τους κινδύνους που έχουν αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας·

β) παρέχουν τα επιθυμητά αποτελέσματα και αυξάνουν την αποδοτικότητα για την ανάπτυξη των συστημάτων ηλεκτρικής ενέργειας·

γ) είναι αποδοτικές και ενταγμένες στο σύνολο των δημόσιων συμβάσεων περιουσιακών στοιχείων και υπηρεσιών.

3. Για την ανάλυση συγκριτικής αξιολόγησης, οι εθνικές ρυθμιστικές αρχές μπορούν να λαμβάνουν υπόψη τον μη δεσμευτικό οδηγό συγκριτικής αξιολόγησης της κυβερνοασφάλειας που έχει καταρτίσει ο ACER και αξιολογούν ειδικότερα:

α) τις μέσες δαπάνες που σχετίζονται με την κυβερνοασφάλεια για τον μετριασμό των κινδύνων που έχουν αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας, ιδίως όσον αφορά τις οντότητες υψηλού αντικτύπου και τις οντότητες κρίσιμου αντικτύπου·

β) σε συνεργασία με το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, τις μέσες τιμές των υπηρεσιών, συστημάτων και προϊόντων κυβερνοασφάλειας που συμβάλλουν σε μεγάλο βαθμό στην ενίσχυση και στη διατήρηση των μέτρων διαχείρισης των κινδύνων για την κυβερνοασφάλεια στις διάφορες λειτουργικές περιφέρειες του συστήματος·

γ) την ύπαρξη και το επίπεδο συγκρισιμότητας του κόστους και των λειτουργιών των υπηρεσιών, συστημάτων και λύσεων κυβερνοασφάλειας που είναι κατάλληλα για την εφαρμογή του παρόντος κανονισμού, προσδιορίζοντας πιθανά μέτρα που είναι αναγκαία για την ενίσχυση της αποδοτικότητας των δαπανών, ιδίως όταν ενδέχεται να απαιτούνται τεχνολογικές επενδύσεις στον τομέα της κυβερνοασφάλειας.

4. Ο χειρισμός και η επεξεργασία όλων των πληροφοριών που σχετίζονται με την ανάλυση συγκριτικής αξιολόγησης πραγματοποιούνται σύμφωνα με τις απαιτήσεις ταξινόμησης δεδομένων του παρόντος κανονισμού, τους ελάχιστους ελέγχους κυβερνοασφάλειας και την έκθεση εκτίμησης κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η ανάλυση συγκριτικής αξιολόγησης που αναφέρεται στις παραγράφους 2 και 3 δεν δημοσιοποιείται.

5. Με την επιφύλαξη των απαιτήσεων εμπιστευτικότητας του άρθρου 47 και της ανάγκης προστασίας της ασφάλειας των οντοτήτων που υπόκεινται στις διατάξεις του παρόντος κανονισμού, η ανάλυση συγκριτικής αξιολόγησης που αναφέρεται στις παραγράφους 2 και 3 του παρόντος άρθρου κοινοποιείται σε όλες τις εθνικές ρυθμιστικές αρχές, σε όλες τις αρμόδιες αρχές, στον ACER, στον ENISA και στην Επιτροπή.

Άρθρο 14

Συμφωνίες με ΔΣΜ από χώρες εκτός της Ένωσης

1. Εντός 18 μηνών από την έναρξη ισχύος του παρόντος κανονισμού, οι ΔΣΜ μιας λειτουργικής περιφέρειας συστήματος που γειτνιάζει με τρίτη χώρα επιδιώκουν τη σύναψη συμφωνιών με τους ΔΣΜ της γειτονικής τρίτης χώρας, οι οποίες είναι σύμφωνες με το σχετικό δίκαιο της Ένωσης και καθορίζουν τη βάση συνεργασίας όσον αφορά την προστασία της κυβερνοασφάλειας και τις ρυθμίσεις συνεργασίας στον τομέα της κυβερνοασφάλειας με τους εν λόγω ΔΣΜ.

2. Οι ΔΣΜ ενημερώνουν την αρμόδια αρχή για τις συμφωνίες που συνάπτονται σύμφωνα με την παράγραφο 1.

Άρθρο 15

Νόμιμοι εκπρόσωποι

1. Οι οντότητες που δεν έχουν εγκατάσταση στην Ένωση, αλλά παρέχουν υπηρεσίες σε οντότητες στην Ένωση και έχουν λάβει κοινοποίηση ότι χαρακτηρίζονται ως οντότητες υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 ορίζουν εγγράφως, εντός τριών μηνών από την ειδοποίηση, εκπρόσωπο στην Ένωση και ενημερώνουν σχετικά την αρμόδια αρχή που απέστειλε τη σχετική κοινοποίηση.

2. Ο εκπρόσωπος αυτός λαμβάνει την εντολή να αποτελεί σημείο επικοινωνίας για οποιαδήποτε αρμόδια αρχή ή CSIRT στην Ένωση επιπρόσθετα στην οντότητα υψηλού ή κρίσιμου αντικτύπου, ή αντ' αυτής, όσον αφορά τις υποχρεώσεις της οντότητας δυνάμει του παρόντος κανονισμού. Η οντότητα υψηλού ή κρίσιμου αντικτύπου παρέχει στον νόμιμο εκπρόσωπό της τις αναγκαίες εξουσίες και επαρκείς πόρους για τη διασφάλιση της αποδοτικής και έγκαιρης συνεργασίας του με τις σχετικές αρμόδιες αρχές ή τις CSIRT.

3. Ο εκπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη μέλη στα οποία η οντότητα παρέχει τις υπηρεσίες της. Η οντότητα θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εκπρόσωπος. Οι οντότητες υψηλού ή κρίσιμου αντικτύπου κοινοποιούν το όνομα, την ταχυδρομική διεύθυνση, τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον αριθμό τηλεφώνου του νόμιμου εκπροσώπου τους στην αρμόδια αρχή στο κράτος μέλος στο οποίο διαμένει ή είναι εγκατεστημένος ο εν λόγω νόμιμος εκπρόσωπος.

4. Ο οριοθείς νόμιμος εκπρόσωπος μπορεί να θεωρηθεί υπεύθυνος για τη μη συμμόρφωση με υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό, με την επιφύλαξη της ευθύνης και των νομικών ενεργειών που μπορεί να κινηθούν κατά της ίδιας της οντότητας υψηλού ή κρίσιμου αντικτύπου.

5. Εάν δεν έχει οριστεί εκπρόσωπος εντός της Ένωσης δυνάμει του παρόντος άρθρου, κάθε κράτος μέλος στο οποίο η οντότητα παρέχει υπηρεσίες μπορεί να κινήσει νομικές διαδικασίες κατά της οντότητας για μη συμμόρφωση με τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό.

6. Ο ορισμός νόμιμου εκπροσώπου εντός της Ένωσης σύμφωνα με την παράγραφο 1 δεν συνιστά εγκατάσταση στην Ένωση.

Άρθρο 16

Συνεργασία μεταξύ του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ

1. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ συνεργάζονται για τη διενέργεια εκτιμήσεων κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 19 και το άρθρο 21, και ειδικότερα για την εκτέλεση των παρακάτω καθηκόντων:

α) ανάπτυξη των μεθοδολογιών εκτίμησης κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 18 παράγραφος 1·

β) εκπόνηση της συνολικής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας σύμφωνα με το άρθρο 23·

γ) ανάπτυξη του κοινού πλαισίου κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας σύμφωνα με το κεφάλαιο III·

δ) κατάρτιση της σύστασης για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 35·

ε) ανάπτυξη της μεθοδολογίας για την κλίμακα ταξινόμησης κυβερνοεπιθέσεων σύμφωνα με το άρθρο 37 παράγραφος 8·

στ) εκπόνηση του προσωρινού δείκτη αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας (στο εξής: ECII) σύμφωνα με το άρθρο 48 παράγραφος 1 στοιχείο α)·

ζ) κατάρτιση του ενοποιημένου προσωρινού καταλόγου οντοτήτων υψηλού αντικτύπου και οντοτήτων κρίσιμου αντικτύπου σύμφωνα με το άρθρο 48 παράγραφος 3·

η) κατάρτιση του προσωρινού καταλόγου διαδικασιών υψηλού αντικτύπου και διαδικασιών κρίσιμου αντικτύπου σε επίπεδο Ένωσης σύμφωνα με το άρθρο 48 παράγραφος 4·

θ) κατάρτιση του προσωρινού καταλόγου ευρωπαϊκών και διεθνών προτύπων και ελέγχων σύμφωνα με το άρθρο 48 παράγραφος 6·

ι) διενέργεια της εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19·

ια) διενέργεια των περιφερειακών εκτιμήσεων κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 21·

ιβ) καθορισμό των περιφερειακών σχεδίων μετριασμού των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 22·

ιγ) ανάπτυξη καθοδήγησης σχετικά με τα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, σύμφωνα με το άρθρο 36·

ιδ) κατάρτιση κατευθυντήριων γραμμών για την εφαρμογή του παρόντος κανονισμού σε διαβούλευση με τον ACER και τον ENISA.

2. Η συνεργασία μεταξύ του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ μπορεί να λάβει τη μορφή ομάδας εργασίας για τους κινδύνους για την κυβερνοασφάλεια.

3. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ ενημερώνουν τακτικά τον ACER, τον ENISA, την Ομάδα Συνεργασίας NIS και τη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού σχετικά με την πρόοδο ως προς τη διενέργεια των εκτιμήσεων κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης και σε περιφερειακό επίπεδο σύμφωνα με το άρθρο 19 και το άρθρο 21.

Άρθρο 17

Συνεργασία μεταξύ του ACER και των αρμόδιων αρχών

Ο ACER, σε συνεργασία με κάθε αρμόδια αρχή:

1) παρακολουθεί την εφαρμογή των μέτρων διαχείρισης κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 12 παράγραφος 2 στοιχείο α) και τις υποχρεώσεις υποβολής εκθέσεων σύμφωνα με το άρθρο 27 και το άρθρο 39· και

2) παρακολουθεί τη διαδικασία έγκρισης και την εφαρμογή των όρων και προϋποθέσεων, των μεθοδολογιών ή των σχεδίων σύμφωνα με το άρθρο 6 παράγραφοι 2 και 3. Η συνεργασία μεταξύ του ACER, του ENISA και κάθε αρμόδιας αρχής μπορεί να λάβει τη μορφή φορέα παρακολούθησης των κινδύνων για την κυβερνοασφάλεια.

ΚΕΦΑΛΑΙΟ ΙΙ

ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ ΚΑΙ ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΩΝ ΣΧΕΤΙΚΩΝ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Άρθρο 18

Μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια

1. Έως τις 13ης Μαρτίου 2025 οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και αφού ζητήσουν τη γνώμη της Ομάδας Συνεργασίας NIS, υποβάλλουν πρόταση για τις μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, σε περιφερειακό επίπεδο και σε επίπεδο κρατών μελών.

2. Οι μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, σε περιφερειακό επίπεδο και σε επίπεδο κρατών μελών περιλαμβάνουν:

α) κατάλογο των κυβερνοαπειλών που πρέπει να λαμβάνονται υπόψη, συμπεριλαμβανομένων τουλάχιστον των ακόλουθων απειλών στην αλυσίδα εφοδιασμού:

i) σοβαρή και απροσδόκητη διαταραχή της αλυσίδας εφοδιασμού·

ii) μη διαθεσιμότητα προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ από την αλυσίδα εφοδιασμού·

iii) κυβερνοεπιθέσεις που δρομολογούνται μέσω παραγόντων της αλυσίδας εφοδιασμού·

iv) διαρροή ευαίσθητων πληροφοριών μέσω της αλυσίδας εφοδιασμού, συμπεριλαμβανομένης της παρακολούθησης της αλυσίδας εφοδιασμού·

v) εισαγωγή αδυναμιών ή κερκόπορτων σε προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ ή διαδικασίες ΤΠΕ μέσω παραγόντων της αλυσίδας εφοδιασμού·

β) τα κριτήρια για την αξιολόγηση του αντικτύπου των κινδύνων για την κυβερνοασφάλεια ως υψηλού ή κρίσιμου, με τη χρήση καθορισμένων ορίων για τις συνέπειες και την πιθανότητα·

γ) προσέγγιση για την ανάλυση των κινδύνων για την κυβερνοασφάλεια που απορρέουν από παρωχημένα συστήματα, τις αλυσιδωτές επιπτώσεις των κυβερνοεπιθέσεων και τον χαρακτήρα πραγματικού χρόνου των συστημάτων που διατηρούν σε λειτουργία το δίκτυο·

δ) προσέγγιση για την ανάλυση των κινδύνων για την κυβερνοασφάλεια που απορρέουν από την εξάρτηση από έναν μόνο προμηθευτή προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ ή διαδικασιών ΤΠΕ.

3. Οι μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, σε περιφερειακό επίπεδο και σε επίπεδο κρατών μελών αξιολογούν τους κινδύνους για την κυβερνοασφάλεια με τη χρήση του ίδιου πίνακα αντικτύπου κινδύνων. Ο πίνακας αντικτύπου κινδύνων:

α) μετρά τις συνέπειες των κυβερνοεπιθέσεων με βάση τα ακόλουθα κριτήρια:

i) απώλεια φορτίου·

ii) μείωση της παραγωγής ηλεκτρικής ενέργειας·

iii) απώλεια δυναμικότητας στην πρωτεύουσα εφεδρεία συχνότητας·

iv) απώλεια δυναμικότητας για την αποκατάσταση της λειτουργίας ηλεκτρικού δικτύου χωρίς εξάρτηση από το εξωτερικό δίκτυο μεταφοράς για την ανάκαμψη μετά από ολική ή μερική παύση λειτουργίας (αποκαλούμενη επίσης «επανεκκίνηση από ολική διακοπή»)·

v) την αναμενόμενη διάρκεια διακοπής ηλεκτρικής ενέργειας που επηρεάζει τους πελάτες σε συνδυασμό με την κλίμακα της διακοπής σε αριθμούς πελατών· και

vi) κάθε άλλο ποσοτικό ή ποιοτικό κριτήριο που θα μπορούσε εύλογα να χρησιμεύσει ως δείκτης των επιπτώσεων μιας κυβερνοεπίθεσης στις διασυνοριακές ροές ηλεκτρικής ενέργειας·

β) μετρά την πιθανότητα εμφάνισης περιστατικού ως τη συχνότητα κυβερνοεπιθέσεων ανά έτος.

4. Οι μεθοδολογίες εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης περιγράφουν τον τρόπο με τον οποίο θα καθοριστούν οι τιμές ECII για τα όρια υψηλού και κρίσιμου αντικτύπου. Ο ECII παρέχει στις οντότητες τη δυνατότητα να αξιολογούν, με τη βοήθεια των κριτηρίων που αναφέρονται στην παράγραφο 2 στοιχείο β), τον αντίκτυπο των κινδύνων στην επιχειρηματική τους διαδικασία κατά τη διάρκεια των εκτιμήσεων αντικτύπου στις επιχειρηματικές δραστηριότητες τις οποίες διενεργούν σύμφωνα με το άρθρο 26 παράγραφος 4 στοιχείο γ) σημείο i).

5. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συντονισμό με τον φορέα ΔΣΔ της ΕΕ, ενημερώνει τη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού σχετικά με τις προτάσεις για τις μεθοδολογίες εκτίμησης κινδύνων για την κυβερνοασφάλεια που εκπονούνται σύμφωνα με την παράγραφο 1.

Άρθρο 19

Εκτίμηση κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης

1. Εντός 9 μηνών από την έγκριση των μεθοδολογιών εκτίμησης των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 8 και, στη συνέχεια, ανά τριετία, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με την Ομάδα Συνεργασίας NIS, διενεργεί, με την επιφύλαξη του άρθρου 22 της οδηγίας (ΕΕ) 2022/2555, εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης και καταρτίζει σχέδιο έκθεσης εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης. Για τον σκοπό αυτόν, θα χρησιμοποιεί τις μεθοδολογίες που έχουν αναπτυχθεί σύμφωνα με το άρθρο 18 και έχουν εγκριθεί σύμφωνα με το άρθρο 8 για τον προσδιορισμό, την ανάλυση και την αξιολόγηση των πιθανών συνεπειών κυβερνοεπιθέσεων που επηρεάζουν την επιχειρησιακή ασφάλεια του συστήματος ηλεκτρικής ενέργειας και διαταράσσουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης δεν λαμβάνει υπόψη τη νομική ή οικονομική ζημία ή τη ζημία στη φήμη που προκαλούν οι κυβερνοεπιθέσεις.

2. Η έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης περιλαμβάνει τα ακόλουθα στοιχεία:

α) τις διαδικασίες υψηλού αντικτύπου σε επίπεδο Ένωσης και τις διαδικασίες κρίσιμου αντικτύπου σε επίπεδο Ένωσης·

β) πίνακα αντικτύπου κινδύνων τον οποίο χρησιμοποιούν οι οντότητες και οι αρμόδιες αρχές για την αξιολόγηση του κινδύνου για την κυβερνοασφάλεια που προσδιορίζεται στην εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους, η οποία διενεργείται σύμφωνα με το άρθρο 20, και στην εκτίμηση κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας σύμφωνα με το άρθρο 26 παράγραφος 2 στοιχείο β).

3. Όσον αφορά τις διαδικασίες υψηλού αντικτύπου σε επίπεδο Ένωσης και τις διαδικασίες κρίσιμου αντικτύπου σε επίπεδο Ένωσης, η έκθεση εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης περιλαμβάνει:

α) εκτίμηση των πιθανών συνεπειών κυβερνοεπίθεσης με τη χρήση των μετρήσεων που ορίζονται στη μεθοδολογία εκτίμησης κινδύνων για την κυβερνοασφάλεια που έχει αναπτυχθεί σύμφωνα με το άρθρο 18 παράγραφοι 2, 3 και 4 και έχει εγκριθεί σύμφωνα με το άρθρο 8·

β) τον ECII και τα όρια υψηλού και κρίσιμου αντικτύπου που χρησιμοποιούν οι αρμόδιες αρχές σύμφωνα με το άρθρο 24 παράγραφοι 1 και 2 για τον προσδιορισμό οντοτήτων υψηλού και κρίσιμου αντικτύπου που συμμετέχουν στις διαδικασίες υψηλού αντικτύπου σε επίπεδο Ένωσης και στις διαδικασίες κρίσιμου αντικτύπου σε επίπεδο Ένωσης.

4. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, υποβάλλει στον ACER προς γνωμοδότηση το σχέδιο της έκθεσης εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης με τα αποτελέσματα της εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης. Ο ACER εκδίδει γνωμοδότηση επί του σχεδίου έκθεσης εντός τριών μηνών από την παραλαβή του. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ λαμβάνουν ιδιαιτέρως υπόψη τη γνωμοδότηση του ACER κατά την οριστικοποίηση της εν λόγω έκθεσης.

5. Εντός τριών μηνών από την παραλαβή της γνωμοδότησης του ACER, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, κοινοποιεί την τελική έκθεση εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης στον ACER, στην Επιτροπή, στον ENISA και στις αρμόδιες αρχές.

Άρθρο 20

Εκτίμηση κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους

1. Κάθε αρμόδια αρχή διενεργεί εκτίμηση των κινδύνων για την κυβερνοασφάλεια στο κράτος μέλος για όλες τις οντότητες υψηλού ή κρίσιμου αντικτύπου στο οικείο κράτος μέλος χρησιμοποιώντας τις μεθοδολογίες που έχουν αναπτυχθεί σύμφωνα με το άρθρο 18 και έχουν εγκριθεί σύμφωνα με το άρθρο 8. Η εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους εντοπίζει και αναλύει τους κινδύνους κυβερνοεπιθέσεων που επηρεάζουν την επιχειρησιακή ασφάλεια του συστήματος ηλεκτρικής ενέργειας με αποτέλεσμα να διαταράσσουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους δεν λαμβάνει υπόψη τη νομική ή οικονομική ζημία ή τη ζημία στη φήμη που προκαλούν οι κυβερνοεπιθέσεις.

2. Εντός 21 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και ανά τριετία μετά την εν λόγω ημερομηνία, και κατόπιν διαβούλευσης με την ΕΑΑ κυβερνοασφάλειας που είναι υπεύθυνη για την ηλεκτρική ενέργεια, κάθε αρμόδια αρχή, με την υποστήριξη της CSIRT, υποβάλλει στο ΕΔΔΣΜ ηλεκτρικής ενέργειας και στον φορέα ΔΣΔ της ΕΕ έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους, η οποία περιέχει τις ακόλουθες πληροφορίες για κάθε επιχειρηματική διαδικασία υψηλού ή κρίσιμου αντικτύπου:

α) την κατάσταση εφαρμογής των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας σύμφωνα με το άρθρο 29·

β) κατάλογο όλων των κυβερνοεπιθέσεων που αναφέρθηκαν κατά τα προηγούμενα τρία έτη σύμφωνα με το άρθρο 38 παράγραφος 3·

γ) σύνοψη των πληροφοριών για τις κυβερνοαπειλές που αναφέρθηκαν κατά τα προηγούμενα τρία έτη σύμφωνα με το άρθρο 38 παράγραφος 6·

δ) για κάθε διαδικασία υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης, εκτίμηση των κινδύνων παραβίασης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των σχετικών περιουσιακών στοιχείων·

ε) όπου απαιτείται, κατάλογο πρόσθετων οντοτήτων που χαρακτηρίζονται ως υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφοι 1, 2, 3 και 5.

3. Η έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους λαμβάνει υπόψη το σχέδιο ετοιμότητας αντιμετώπισης κινδύνων του κράτους μέλους που έχει καταρτιστεί σύμφωνα με το άρθρο 10 του κανονισμού (ΕΕ) 2019/941.

4. Οι πληροφορίες που περιέχονται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους σύμφωνα με την παράγραφο 2 στοιχεία α) έως δ) δεν συνδέονται με συγκεκριμένες οντότητες ή συγκεκριμένα περιουσιακά στοιχεία. Η έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους περιλαμβάνει επίσης εκτίμηση των κινδύνων που εγείρονται από προσωρινές παρεκκλίσεις που εκδίδονται από τις αρμόδιες αρχές των κρατών μελών σύμφωνα με το άρθρο 30.

5. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ μπορούν να ζητούν πρόσθετες πληροφορίες από τις αρμόδιες αρχές σε σχέση με τα καθήκοντα που προσδιορίζονται στην παράγραφο 2 στοιχεία α) και γ).

6. Οι αρμόδιες αρχές διασφαλίζουν ότι οι πληροφορίες που παρέχουν είναι ακριβείς και ορθές.

Άρθρο 21

Περιφερειακές εκτιμήσεις κινδύνων για την κυβερνοασφάλεια

1. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με το σχετικό περιφερειακό συντονιστικό κέντρο, διενεργεί περιφερειακή εκτίμηση των κινδύνων για την κυβερνοασφάλεια για κάθε λειτουργική περιφέρεια του συστήματος χρησιμοποιώντας τις μεθοδολογίες που έχουν αναπτυχθεί σύμφωνα με το άρθρο 19 και έχουν εγκριθεί σύμφωνα με το άρθρο 8, για τον εντοπισμό, την ανάλυση και την αξιολόγηση των κινδύνων κυβερνοεπιθέσεων που επηρεάζουν την επιχειρησιακή ασφάλεια του συστήματος ηλεκτρικής ενέργειας και διαταράσσουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η περιφερειακή εκτίμηση των κινδύνων για την κυβερνοασφάλεια δεν λαμβάνει υπόψη τη νομική ή οικονομική ζημία ή τη ζημία στη φήμη που προκαλούν οι κυβερνοεπιθέσεις.

2. Εντός 30 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και, στη συνέχεια, ανά τριετία, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με την Ομάδα Συνεργασίας NIS, καταρτίζει περιφερειακή έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια για κάθε λειτουργική περιφέρεια του συστήματος.

3. Η περιφερειακή έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια λαμβάνει υπόψη τις σχετικές πληροφορίες που περιέχονται στις εκθέσεις εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης και στις εκθέσεις εκτίμησης των κινδύνων για την κυβερνοασφάλεια των κρατών μελών.

4. Η περιφερειακή εκτίμηση των κινδύνων για την κυβερνοασφάλεια εξετάζει τα περιφερειακά σενάρια κρίσης ηλεκτρικής ενέργειας που σχετίζονται με την κυβερνοασφάλεια, τα οποία προσδιορίζονται σύμφωνα με το άρθρο 6 του κανονισμού (ΕΕ) 2019/941.

Άρθρο 22

Περιφερειακά σχέδια μετριασμού των κινδύνων για την κυβερνοασφάλεια

1. Εντός 36 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και το αργότερο έως τις 13 Ιουνίου 2031, και ανά τριετία στη συνέχεια, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με τα περιφερειακά συντονιστικά κέντρα και την Ομάδα Συνεργασίας NIS, εκπονούν περιφερειακό σχέδιο μετριασμού των κινδύνων για την κυβερνοασφάλεια για κάθε λειτουργική περιφέρεια του συστήματος.

2. Τα περιφερειακά σχέδια μετριασμού των κινδύνων για την κυβερνοασφάλεια περιλαμβάνουν:

α) τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας που εφαρμόζουν οι οντότητες υψηλού ή κρίσιμου αντικτύπου στη λειτουργική περιφέρεια του συστήματος·

β) τους υπολειπόμενους κινδύνους για την κυβερνοασφάλεια στις λειτουργικές περιφέρειες του συστήματος μετά την εφαρμογή των ελέγχων που αναφέρονται στο στοιχείο α).

3. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας υποβάλλει τα περιφερειακά σχέδια μετριασμού των κινδύνων στους σχετικούς διαχειριστές συστημάτων μεταφοράς, στις αρμόδιες αρχές και στη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού. Η Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού μπορεί να προτείνει τροποποιήσεις.

4. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με την Ομάδα Συνεργασίας NIS, επικαιροποιούν τα περιφερειακά σχέδια μετριασμού των κινδύνων ανά τριετία, εκτός εάν οι περιστάσεις απαιτούν συχνότερες επικαιροποιήσεις.

Άρθρο 23

Συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας

1. Εντός 40 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και, στη συνέχεια, ανά τριετία, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με την Ομάδα Συνεργασίας NIS, υποβάλλουν στη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού έκθεση σχετικά με το αποτέλεσμα της αξιολόγησης των κινδύνων για την κυβερνοασφάλεια όσον αφορά τις διασυνοριακές ροές ηλεκτρικής ενέργειας (στο εξής: συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας).

2. Η συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας βασίζεται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, στις εκθέσεις εκτίμησης των κινδύνων για την κυβερνοασφάλεια των κρατών μελών και στις περιφερειακές εκθέσεις εκτίμησης των κινδύνων για την κυβερνοασφάλεια, και περιλαμβάνει τις ακόλουθες πληροφορίες:

α) τον κατάλογο των διαδικασιών υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης που έχουν προσδιοριστεί στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 2 στοιχείο α), συμπεριλαμβανομένης εκτίμησης της πιθανότητας και του αντικτύπου των κινδύνων για την κυβερνοασφάλεια που αξιολογήθηκαν στο πλαίσιο των περιφερειακών εκθέσεων εκτίμησης των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 21 παράγραφος 2 και το άρθρο 19 παράγραφος 3 στοιχείο α)·

β) υφιστάμενες κυβερνοαπειλές, με ιδιαίτερη έμφαση στις αναδυόμενες απειλές και στους αναδυόμενους κινδύνους για το σύστημα ηλεκτρικής ενέργειας·

γ) κυβερνοεπιθέσεις κατά την προηγούμενη περίοδο σε επίπεδο Ένωσης, με κριτική επισκόπηση του τρόπου με τον οποίο οι εν λόγω κυβερνοεπιθέσεις ενδέχεται να είχαν αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας·

δ) τη συνολική κατάσταση εφαρμογής των μέτρων κυβερνοασφάλειας·

ε) την κατάσταση εφαρμογής των ροών πληροφόρησης σύμφωνα με τα άρθρα 37 και 38·

στ) κατάλογο πληροφοριών ή συγκεκριμένα κριτήρια για τη διαβάθμιση των πληροφοριών σύμφωνα με το άρθρο 46·

ζ) κινδύνους που έχουν εντοπιστεί και επισημανθεί, οι οποίοι ενδέχεται να προκύψουν από την επισφαλή διαχείριση της αλυσίδας εφοδιασμού·

η) αποτελέσματα και συσσωρευμένη πείρα από περιφερειακές και διαπεριφερειακές ασκήσεις κυβερνοασφάλειας που διοργανώνονται σύμφωνα με το άρθρο 44·

θ) ανάλυση της εξέλιξης των συνολικών κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας μετά τις τελευταίες περιφερειακές εκτιμήσεις των κινδύνων για την κυβερνοασφάλεια·

ι) κάθε άλλη πληροφορία που μπορεί να είναι χρήσιμη για τον προσδιορισμό πιθανών βελτιώσεων του παρόντος κανονισμού ή της ανάγκης αναθεώρησης του παρόντος κανονισμού ή οποιουδήποτε από τα εργαλεία του· και

ια) συγκεντρωτικές και ανωνυμοποιημένες πληροφορίες σχετικά με παρεκκλίσεις που χορηγήθηκαν σύμφωνα με το άρθρο 30 παράγραφος 3.

3. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 μπορούν να συμβάλλουν στην εκπόνηση της συνολικής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας, με σεβασμό στην εμπιστευτικότητα των πληροφοριών σύμφωνα με το άρθρο 47. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, ζητούν τη γνώμη των εν λόγω οντοτήτων σε πρώιμο στάδιο.

4. Η συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας υπόκειται στους κανόνες για την προστασία της ανταλλαγής πληροφοριών σύμφωνα με το άρθρο 46. Με την επιφύλαξη του άρθρου 10 παράγραφος 4 και του άρθρου 47 παράγραφος 4, το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ δημοσιοποιούν έκδοση της εν λόγω έκθεσης η οποία δεν περιέχει πληροφορίες που μπορούν να προκαλέσουν ζημία σε οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1. Η δημόσια έκδοση της έκθεσης αυτής εκδίδεται μόνο με τη συμφωνία της Ομάδας Συνεργασίας NIS και της Συντονιστικής Ομάδας στον τομέα του Ηλεκτρισμού. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συντονισμό με τον φορέα ΔΣΔ της ΕΕ, είναι υπεύθυνο για τη σύνταξη και τη δημοσίευση της δημόσιας έκδοσης της έκθεσης.

Άρθρο 24

Προσδιορισμός οντοτήτων υψηλού ή κρίσιμου αντικτύπου

1. Κάθε αρμόδια αρχή προσδιορίζει, χρησιμοποιώντας τον ECII και τα όρια υψηλού και κρίσιμου αντικτύπου που περιλαμβάνονται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 3 στοιχείο β), τις οντότητες υψηλού ή κρίσιμου αντικτύπου στο οικείο κράτος μέλος που συμμετέχουν στις διαδικασίες υψηλού και κρίσιμου αντικτύπου σε επίπεδο Ένωσης. Οι αρμόδιες αρχές μπορούν να ζητήσουν πληροφορίες από οντότητα στο οικείο κράτος μέλος για να καθορίσουν τις τιμές του ECII για την εν λόγω οντότητα. Εάν η καθορισμένη τιμή ECII μιας οντότητας υπερβαίνει το όριο υψηλού ή κρίσιμου αντικτύπου, η προσδιορισμένη οντότητα περιλαμβάνεται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους που αναφέρεται στο άρθρο 20 παράγραφος 2.

2. Κάθε αρμόδια αρχή προσδιορίζει, χρησιμοποιώντας τον ECII και τα όρια υψηλού και κρίσιμου αντικτύπου που περιλαμβάνονται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 3 στοιχείο β), τις οντότητες υψηλού ή κρίσιμου αντικτύπου που δεν είναι εγκατεστημένες στην Ένωση, στον βαθμό που δραστηριοποιούνται εντός της Ένωσης. Η αρμόδια αρχή μπορεί να ζητήσει πληροφορίες από οντότητα που δεν είναι εγκατεστημένη στην Ένωση για να καθορίσει τις τιμές ECII για την εν λόγω οντότητα.

3. Κάθε αρμόδια αρχή μπορεί να προσδιορίζει πρόσθετες οντότητες στο οικείο κράτος μέλος ως οντότητες υψηλού ή κρίσιμου αντικτύπου, εάν πληρούνται τα ακόλουθα κριτήρια:

α) η οντότητα αποτελεί μέρος ομάδας οντοτήτων που κινδυνεύουν σημαντικά να επηρεαστούν ταυτόχρονα από κυβερνοεπίθεση·

β) ο ECII συγκεντρωτικά για την ομάδα οντοτήτων υπερβαίνει το όριο υψηλού ή κρίσιμου αντικτύπου.

4. Εάν μια αρμόδια αρχή προσδιορίσει πρόσθετες οντότητες σύμφωνα με την παράγραφο 3, όλες οι διαδικασίες στις εν λόγω οντότητες για τις οποίες ο ECII συγκεντρωτικά για την ομάδα υπερβαίνει το όριο υψηλού αντικτύπου θεωρούνται διαδικασίες υψηλού αντικτύπου και όλες οι διαδικασίες στις εν λόγω οντότητες για τις οποίες ο ECII συγκεντρωτικά για την ομάδα υπερβαίνει τα όρια κρίσιμου αντικτύπου θεωρούνται διαδικασίες κρίσιμου αντικτύπου.

5. Εάν μια αρμόδια αρχή προσδιορίσει οντότητες που αναφέρονται στην παράγραφο 3 στοιχείο α) σε περισσότερα από ένα κράτη μέλη, ενημερώνει τις άλλες αρμόδιες αρχές, το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, με βάση τις πληροφορίες που λαμβάνει από όλες τις αρμόδιες αρχές, παρέχει στις αρμόδιες αρχές ανάλυση της συγκέντρωσης οντοτήτων σε περισσότερα από ένα κράτη μέλη που μπορεί να προκαλέσει κατανεμημένη διατάραξη στις διασυνοριακές ροές ηλεκτρικής ενέργειας και μπορεί να οδηγήσει σε κυβερνοεπίθεση. Όταν μια ομάδα οντοτήτων σε περισσότερα του ενός κράτη μέλη προσδιορίζεται ως συγκέντρωση της οποίας ο ECII υπερβαίνει το όριο υψηλού ή κρίσιμου αντικτύπου, όλες οι ενδιαφερόμενες αρμόδιες αρχές χαρακτηρίζουν τις οντότητες της εν λόγω ομάδας ως οντότητες υψηλού ή κρίσιμου αντικτύπου για το οικείο αντίστοιχο κράτος μέλος, με βάση τον συγκεντρωτικό ECII για την ομάδα των οντοτήτων, και οι χαρακτηρισμένες αυτές οντότητες αναφέρονται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης.

6. Εντός εννέα μηνών από την κοινοποίηση, από το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, της έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 5 και, σε κάθε περίπτωση, το αργότερο έως τις 13 Ιουνίου 2028, κάθε αρμόδια αρχή ειδοποιεί τις οντότητες του καταλόγου ότι έχουν χαρακτηριστεί οντότητες υψηλού ή κρίσιμου αντικτύπου στο οικείο κράτος μέλος.

7. Όταν ένας πάροχος υπηρεσιών αναφέρεται σε αρμόδια αρχή ως πάροχος κρίσιμων υπηρεσιών ΤΠΕ σύμφωνα με το άρθρο 27 στοιχείο γ), η εν λόγω αρμόδια αρχή ειδοποιεί σχετικά τις αρμόδιες αρχές των κρατών μελών στο έδαφος των οποίων βρίσκεται η έδρα ή ο εκπρόσωπος. Οι εν λόγω τελευταίες αρμόδιες αρχές ενημερώνουν τον πάροχο υπηρεσιών ότι έχει χαρακτηριστεί πάροχος κρίσιμων υπηρεσιών.

Άρθρο 25

Εθνικά συστήματα επαλήθευσης

1. Οι αρμόδιες αρχές μπορούν να θεσπίσουν εθνικό σύστημα επαλήθευσης για να επαληθεύουν ότι οι οντότητες κρίσιμου αντικτύπου που προσδιορίζονται σύμφωνα με το άρθρο 24 παράγραφος 1 εφαρμόζουν το εθνικό νομοθετικό πλαίσιο το οποίο περιλαμβάνεται στον πίνακα χαρτογράφησης που αναφέρεται στο άρθρο 34. Το εθνικό σύστημα επαλήθευσης μπορεί να βασίζεται σε επιθεώρηση που διενεργείται από την αρμόδια αρχή, σε ανεξάρτητους ελέγχους ασφάλειας ή σε αμοιβαίες αξιολογήσεις από ομοτίμους από οντότητες κρίσιμου αντικτύπου στο ίδιο κράτος μέλος, υπό την εποπτεία της αρμόδιας αρχής.

2. Εάν μια αρμόδια αρχή αποφασίσει να θεσπίσει εθνικό σύστημα επαλήθευσης, η εν λόγω αρμόδια αρχή διασφαλίζει ότι η επαλήθευση διενεργείται σύμφωνα με τις ακόλουθες απαιτήσεις:

α) κάθε μέρος που διενεργεί την αξιολόγηση από ομοτίμους, τον έλεγχο ή την επιθεώρηση είναι ανεξάρτητο από την οντότητα κρίσιμου αντικτύπου υπό επαλήθευση και δεν έχει συγκρούσεις συμφερόντων·

β) το προσωπικό που διενεργεί την αξιολόγηση από ομοτίμους, τον έλεγχο ή την επιθεώρηση διαθέτει αποδεδειγμένες γνώσεις σχετικά με:

i) την κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας·

ii) τα συστήματα διαχείρισης της κυβερνοασφάλειας·

iii) τις αρχές του ελέγχου·

iv) την εκτίμηση των κινδύνων για την κυβερνοασφάλεια·

v) το κοινό πλαίσιο κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας·

vi) το εθνικό νομοθετικό και κανονιστικό πλαίσιο και τα ευρωπαϊκά και διεθνή πρότυπα που εμπίπτουν στο πεδίο εφαρμογής της επαλήθευσης·

vii) τις διαδικασίες κρίσιμου αντικτύπου που εμπίπτουν στο πεδίο εφαρμογής της επαλήθευσης·

γ) στο μέρος που διενεργεί την αξιολόγηση από ομοτίμους, τον έλεγχο ή την επιθεώρηση παρέχεται επαρκής χρόνος για την εκτέλεση των εν λόγω δραστηριοτήτων·

δ) το μέρος που διενεργεί την αξιολόγηση από ομοτίμους, τον έλεγχο ή την επιθεώρηση λαμβάνει τα κατάλληλα μέτρα για την προστασία των πληροφοριών που συλλέγει κατά την επαλήθευση, σύμφωνα με το επίπεδο εμπιστευτικότητάς τους· και

ε) οι αξιολογήσεις από ομοτίμους, οι έλεγχοι ή οι επιθεωρήσεις διενεργούνται τουλάχιστον μία φορά ετησίως και καλύπτουν το πλήρες πεδίο εφαρμογής της επαλήθευσης τουλάχιστον ανά τριετία.

3. Εάν μια αρμόδια αρχή αποφασίσει να θεσπίσει εθνικό σύστημα επαλήθευσης, υποβάλλει έκθεση στον ACER σε ετήσια βάση σχετικά με τη συχνότητα διενέργειας επιθεωρήσεων στο πλαίσιο του εν λόγω συστήματος.

Άρθρο 26

Διαχείριση κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας

1. Κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου, όπως προσδιορίζεται από τις αρμόδιες αρχές σύμφωνα με το άρθρο 24 παράγραφος 1, εκτελεί τη διαχείριση των κινδύνων για την κυβερνοασφάλεια για όλα τα περιουσιακά στοιχεία της στις οικείες περιμέτρους υψηλού ή κρίσιμου αντικτύπου. Κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου προβαίνει ανά τριετία σε διαχείριση κινδύνων που περιλαμβάνει τα στάδια της παραγράφου 2.

2. Κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου βασίζει τη διαχείριση των κινδύνων για την κυβερνοασφάλεια σε προσέγγιση που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών της και που περιλαμβάνει τα ακόλουθα στάδια:

α) καθορισμός πλαισίου·

β) εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας·

γ) αντιμετώπιση των κινδύνων για την κυβερνοασφάλεια·

δ) αποδοχή των κινδύνων για την κυβερνοασφάλεια.

3. Κατά το στάδιο καθορισμού του πλαισίου, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου:

α) καθορίζει το πεδίο εφαρμογής της εκτίμησης των κινδύνων για την κυβερνοασφάλεια, συμπεριλαμβανομένων των διαδικασιών υψηλού ή κρίσιμου αντικτύπου που προσδιορίζονται από το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ, καθώς και άλλων διαδικασιών που ενδέχεται να αποτελούν στόχο κυβερνοεπιθέσεων με υψηλό ή κρίσιμο αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας· και

β) καθορίζει τα κριτήρια για την αξιολόγηση και την αποδοχή των κινδύνων σύμφωνα με τον πίνακα αντικτύπου κινδύνων που χρησιμοποιούν οι οντότητες και οι αρμόδιες αρχές για την εκτίμηση των κινδύνων για την κυβερνοασφάλεια στις μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, σε περιφερειακό επίπεδο και σε επίπεδο κράτους μέλους, οι οποίες αναπτύσσονται από το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ σύμφωνα με το άρθρο 19 παράγραφος 2.

4. Κατά το στάδιο εκτίμησης των κινδύνων για την κυβερνοασφάλεια, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου:

α) προσδιορίζει τους κινδύνους για την κυβερνοασφάλεια λαμβάνοντας υπόψη:

i) όλα τα περιουσιακά στοιχεία που υποστηρίζουν τις διαδικασίες υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης, με εκτίμηση του πιθανού αντικτύπου στις διασυνοριακές ροές ηλεκτρικής ενέργειας σε περίπτωση που τεθεί σε κίνδυνο το περιουσιακό στοιχείο·

ii) πιθανές κυβερνοαπειλές, λαμβανομένων υπόψη των κυβερνοαπειλών που προσδιορίζονται στην τελευταία συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας που αναφέρεται στο άρθρο 23 και των απειλών στην αλυσίδα εφοδιασμού·

iii) ευπάθειες, συμπεριλαμβανομένων ευπαθειών σε παρωχημένα συστήματα·

iv) πιθανά σενάρια κυβερνοεπιθέσεων, συμπεριλαμβανομένων κυβερνοεπιθέσεων που επηρεάζουν την επιχειρησιακή ασφάλεια του συστήματος ηλεκτρικής ενέργειας και διαταράσσουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας·

v) σχετικές αξιολογήσεις και εκτιμήσεις κινδύνων που διενεργούνται σε επίπεδο Ένωσης, συμπεριλαμβανομένων συντονισμένων εκτιμήσεων κινδύνου για κρίσιμες αλυσίδες εφοδιασμού σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555· και

vi) υφιστάμενους ελέγχους που έχουν πραγματοποιηθεί·

β) αναλύει την πιθανότητα και τις συνέπειες των κινδύνων για την κυβερνοασφάλεια που προσδιορίζονται στο στοιχείο α) και καθορίζει το επίπεδο κινδύνων για την κυβερνοασφάλεια με τη χρήση του πίνακα αντικτύπου κινδύνων που χρησιμοποιείται για την εκτίμηση των κινδύνων για την κυβερνοασφάλεια στις μεθοδολογίες εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, σε περιφερειακό επίπεδο και σε επίπεδο κράτους μέλους, ο οποίος έχει αναπτυχθεί από τους ΔΣΜ με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ σύμφωνα με το άρθρο 19 παράγραφος 2·

γ) κατατάσσει τα περιουσιακά στοιχεία ανάλογα με τις πιθανές συνέπειες σε περίπτωση διακύβευσης της κυβερνοασφάλειας και προσδιορίζει τις περιμέτρους υψηλού ή κρίσιμου αντικτύπου χρησιμοποιώντας τα ακόλουθα βήματα:

i) διενεργεί, για όλες τις διαδικασίες που καλύπτονται από την εκτίμηση των κινδύνων για την κυβερνοασφάλεια, εκτίμηση επιχειρηματικών επιπτώσεων χρησιμοποιώντας τον ΕCII·

ii) κατατάσσει μια διαδικασία ως υψηλού ή κρίσιμου αντικτύπου, εάν ο οικείος ECII υπερβαίνει το όριο υψηλού ή κρίσιμου αντικτύπου, αντίστοιχα·

iii) προσδιορίζει όλα τα περιουσιακά στοιχεία υψηλού ή κρίσιμου αντικτύπου ως τα περιουσιακά στοιχεία που απαιτούνται για τις διαδικασίες υψηλού και κρίσιμου αντικτύπου, αντίστοιχα·

iv) καθορίζει τις περιμέτρους υψηλού ή κρίσιμου αντικτύπου που περικλείουν όλα τα περιουσιακά στοιχεία υψηλού και κρίσιμου αντικτύπου, αντίστοιχα, ώστε να μπορεί να ελέγχεται η πρόσβαση στην περίμετρο·

δ) αξιολογεί τους κινδύνους για την κυβερνοασφάλεια ιεραρχώντας τους μέσω των κριτηρίων αξιολόγησης κινδύνων και των κριτηρίων αποδοχής κινδύνων που αναφέρονται στην παράγραφο 3 στοιχείο β).

5. Κατά το στάδιο αντιμετώπισης των κινδύνων για την κυβερνοασφάλεια, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου καταρτίζει σχέδιο μετριασμού των κινδύνων σε επίπεδο οντότητας επιλέγοντας λύσεις αντιμετώπισης των κινδύνων κατάλληλες για τη διαχείριση των κινδύνων και τον προσδιορισμό των υπολειπόμενων κινδύνων.

6. Κατά το στάδιο αποδοχής των κινδύνων για την κυβερνοασφάλεια, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου αποφασίζει αν θα αποδεχτεί τον υπολειπόμενο κίνδυνο με βάση τα κριτήρια αποδοχής κινδύνων που καθορίζονται στην παράγραφο 3 στοιχείο β).

7. Κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου καταχωρίζει τα περιουσιακά στοιχεία που προσδιορίζονται στην παράγραφο 1 σε κατάλογο απογραφής περιουσιακών στοιχείων. Ο εν λόγω κατάλογος απογραφής περιουσιακών στοιχείων δεν αποτελεί μέρος της έκθεσης εκτίμησης των κινδύνων.

8. Η αρμόδια αρχή μπορεί να επιθεωρεί τα περιουσιακά στοιχεία του καταλόγου απογραφής κατά τη διάρκεια επιθεωρήσεων.

Άρθρο 27

Υποβολή εκθέσεων σχετικά με την εκτίμηση κινδύνων σε επίπεδο οντότητας

Εντός 12 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και, στη συνέχεια, ανά τριετία, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου υποβάλλει στην αρμόδια αρχή έκθεση που περιέχει τις ακόλουθες πληροφορίες:

1) κατάλογο των ελέγχων που επιλέχθηκαν για το σχέδιο μετριασμού των κινδύνων σε επίπεδο οντότητας σύμφωνα με το άρθρο 26 παράγραφος 5 με την τρέχουσα κατάσταση εφαρμογής κάθε ελέγχου·

2) για κάθε διαδικασία υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης, εκτίμηση του κινδύνου παραβίασης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των σχετικών περιουσιακών στοιχείων. Η εκτίμηση του εν λόγω κινδύνου πραγματοποιείται σύμφωνα με τον πίνακα αντικτύπου κινδύνων που αναφέρεται στο άρθρο 19 παράγραφος 2·

3) κατάλογο των παρόχων κρίσιμων υπηρεσιών ΤΠΕ για τις οικείες διαδικασίες κρίσιμου αντικτύπου.

ΚΕΦΑΛΑΙΟ III

ΚΟΙΝΟ ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

Άρθρο 28

Σύνθεση, λειτουργία και επανεξέταση του κοινού πλαισίου κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας

1. Το κοινό πλαίσιο κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας αποτελείται από τους ακόλουθους ελέγχους και το ακόλουθο σύστημα διαχείρισης της κυβερνοασφάλειας:

α) τους ελάχιστους ελέγχους κυβερνοασφάλειας, οι οποίοι έχουν αναπτυχθεί σύμφωνα με το άρθρο 29·

β) τους προηγμένους ελέγχους κυβερνοασφάλειας, οι οποίοι έχουν αναπτυχθεί σύμφωνα με το άρθρο 29·

γ) τον πίνακα χαρτογράφησης, ο οποίος έχει καταρτιστεί σύμφωνα με το άρθρο 34 και στον οποίο χαρτογραφούνται οι έλεγχοι που αναφέρονται στα στοιχεία α) και β) με βάση επιλεγμένα ευρωπαϊκά και διεθνή πρότυπα και εθνικά νομοθετικά ή ρυθμιστικά πλαίσια·

δ) το σύστημα διαχείρισης της κυβερνοασφάλειας που έχει θεσπιστεί σύμφωνα με το άρθρο 32.

2. Όλες οι οντότητες υψηλού αντικτύπου εφαρμόζουν τους ελάχιστους ελέγχους κυβερνοασφάλειας σύμφωνα με την παράγραφο 1 στοιχείο α) εντός της οικείας περιμέτρου υψηλού αντικτύπου.

3. Όλες οι οντότητες κρίσιμου αντικτύπου εφαρμόζουν τους προηγμένους ελέγχους κυβερνοασφάλειας σύμφωνα με την παράγραφο 1 στοιχείο β) εντός της οικείας περιμέτρου κρίσιμου αντικτύπου.

4. Εντός 7 μηνών από την υποβολή του πρώτου σχεδίου έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 4, το κοινό πλαίσιο κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας που αναφέρεται στην παράγραφο 1 συμπληρώνεται από τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας στην αλυσίδα εφοδιασμού που αναπτύσσονται σύμφωνα με το άρθρο 33.

Άρθρο 29

Ελάχιστοι και προηγμένοι έλεγχοι κυβερνοασφάλειας

1. Εντός 7 μηνών από την υποβολή του πρώτου σχεδίου έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 4, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζουν πρόταση για ελάχιστους και προηγμένους ελέγχους κυβερνοασφάλειας.

2. Εντός 6 μηνών από την κατάρτιση κάθε περιφερειακής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 21 παράγραφος 2, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, προτείνουν στην αρμόδια αρχή τροποποίηση των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας. Η πρόταση θα υποβάλλεται σύμφωνα με το άρθρο 8 παράγραφος 10 και θα λαμβάνει υπόψη τους κινδύνους που προσδιορίστηκαν στην περιφερειακή εκτίμηση κινδύνων.

3. Οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας θα μπορούν να επαληθευτούν με τη συμμετοχή σε εθνικό σύστημα επαλήθευσης σύμφωνα με τη διαδικασία που ορίζεται στο άρθρο 31 ή με τη διενέργεια ανεξάρτητων ελέγχων ασφάλειας από τρίτους σύμφωνα με τις απαιτήσεις που αναφέρονται στο άρθρο 25 παράγραφος 2.

4. Οι αρχικοί ελάχιστοι και προηγμένοι έλεγχοι κυβερνοασφάλειας που αναπτύσσονται σύμφωνα με την παράγραφο 1 βασίζονται στους κινδύνους οι οποίοι προσδιορίζονται στην έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης που αναφέρεται στο άρθρο 19 παράγραφος 5. Οι τροποποιημένοι ελάχιστοι και προηγμένοι έλεγχοι κυβερνοασφάλειας που αναπτύσσονται σύμφωνα με την παράγραφο 2 βασίζονται στην περιφερειακή έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια που αναφέρεται στο άρθρο 21 παράγραφος 2.

5. Οι ελάχιστοι έλεγχοι κυβερνοασφάλειας περιλαμβάνουν ελέγχους για την προστασία των πληροφοριών που ανταλλάσσονται σύμφωνα με το άρθρο 46.

6. Εντός 12 μηνών από την έγκριση των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας σύμφωνα με το άρθρο 8 παράγραφος 5, ή μετά από κάθε επικαιροποίηση σύμφωνα με το άρθρο 8 παράγραφος 10, οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 και χαρακτηρίζονται οντότητες κρίσιμου ή υψηλού αντικτύπου σύμφωνα με το άρθρο 24 εφαρμόζουν, κατά την κατάρτιση του σχεδίου μετριασμού των κινδύνων σε επίπεδο οντότητας σύμφωνα με το άρθρο 26 παράγραφος 5, τους ελάχιστους ελέγχους κυβερνοασφάλειας εντός της περιμέτρου υψηλού αντικτύπου και τους προηγμένους ελέγχους κυβερνοασφάλειας εντός της περιμέτρου κρίσιμου αντικτύπου.

Άρθρο 30

Παρεκκλίσεις από τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας

1. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 μπορούν να ζητήσουν από την αντίστοιχη αρμόδια αρχή να χορηγήσει παρέκκλιση από την υποχρέωσή τους να διενεργούν τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας που αναφέρονται στο άρθρο 29 παράγραφος 6. Η αρμόδια αρχή μπορεί να χορηγήσει τέτοια παρέκκλιση για έναν από τους ακόλουθους λόγους:

α) σε εξαιρετικές περιπτώσεις, όταν η οντότητα μπορεί να αποδείξει ότι το κόστος διενέργειας των κατάλληλων ελέγχων κυβερνοασφάλειας υπερβαίνει σημαντικά τα οφέλη. Ο ACER και το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ, μπορούν να αναπτύξουν από κοινού καθοδήγηση για την εκτίμηση του κόστους των ελέγχων κυβερνοασφάλειας, ώστε να βοηθήσουν τις οντότητες·

β) όταν η οντότητα παρέχει σχέδιο αντιμετώπισης των κινδύνων σε επίπεδο οντότητας το οποίο μετριάζει τους κινδύνους για την κυβερνοασφάλεια με τη χρήση εναλλακτικών ελέγχων σε επίπεδο αποδεκτό σύμφωνα με τα κριτήρια αποδοχής κινδύνων που αναφέρονται στο άρθρο 26 παράγραφος 3 στοιχείο β).

2. Εντός τριών μηνών από την παραλαβή του αιτήματος που αναφέρεται στην παράγραφο 1, κάθε αρμόδια αρχή αποφασίζει αν θα χορηγηθεί παρέκκλιση από τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας. Παρεκκλίσεις από τους ελάχιστους ή τους προηγμένους ελέγχους κυβερνοασφάλειας χορηγούνται για μέγιστη περίοδο τριών ετών, με δυνατότητα ανανέωσης.

3. Συγκεντρωτικές και ανωνυμοποιημένες πληροφορίες για τις παρεκκλίσεις που χορηγούνται περιλαμβάνονται με τη μορφή παραρτήματος στη συνολική έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια στις διασυνοριακές ροές ηλεκτρικής ενέργειας που αναφέρεται στο άρθρο 23. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ επικαιροποιούν από κοινού τον κατάλογο, εφόσον απαιτείται.

Άρθρο 31

Επαλήθευση του κοινού πλαισίου κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας

1. Το αργότερο 24 μήνες μετά την έγκριση των ελέγχων που αναφέρονται στο άρθρο 28 παράγραφος 1 στοιχεία α), β) και γ) και τη θέσπιση του συστήματος διαχείρισης της κυβερνοασφάλειας που αναφέρεται στο στοιχείο δ) του εν λόγω άρθρου, κάθε οντότητα κρίσιμου αντικτύπου που προσδιορίζεται σύμφωνα με το άρθρο 24 παράγραφος 1 είναι σε θέση να αποδείξει τη συμμόρφωσή της με το σύστημα διαχείρισης της κυβερνοασφάλειας και τους ελάχιστους ή τους προηγμένους ελέγχους κυβερνοασφάλειας, κατόπιν αιτήματος της αρμόδιας αρχής.

2. Κάθε οντότητα κρίσιμου αντικτύπου εκπληρώνει την υποχρέωση που αναφέρεται στην παράγραφο 1 με την υπαγωγή της σε ανεξάρτητους ελέγχους ασφάλειας από τρίτους σύμφωνα με τις απαιτήσεις που αναφέρονται στο άρθρο 25 παράγραφος 2 ή με τη συμμετοχή της σε εθνικό σύστημα επαλήθευσης σύμφωνα με το άρθρο 25 παράγραφος 1.

3. Η επαλήθευση της συμμόρφωσης μιας οντότητας κρίσιμου αντικτύπου με το σύστημα διαχείρισης της κυβερνοασφάλειας και τους ελάχιστους ή τους προηγμένους ελέγχους κυβερνοασφάλειας καλύπτει όλα τα περιουσιακά στοιχεία εντός της περιμέτρου κρίσιμου αντικτύπου της οντότητας κρίσιμου αντικτύπου.

4. Η επαλήθευση της συμμόρφωσης μιας οντότητας κρίσιμου αντικτύπου με το σύστημα διαχείρισης της κυβερνοασφάλειας και τους ελάχιστους ή τους προηγμένους ελέγχους κυβερνοασφάλειας επαναλαμβάνεται τακτικά, το αργότερο 36 μήνες μετά τη λήξη της πρώτης επαλήθευσης και, στη συνέχεια, ανά 3 έτη.

5. Κάθε οντότητα κρίσιμου αντικτύπου που ορίζεται σύμφωνα με το άρθρο 24 αποδεικνύει τη συμμόρφωσή της με τους ελέγχους που αναφέρονται στο άρθρο 28 παράγραφος 1 στοιχεία α), β) και γ) και τη θέσπιση του συστήματος διαχείρισης της κυβερνοασφάλειας που αναφέρεται στο στοιχείο δ) του εν λόγω άρθρου, υποβάλλοντας στην αρμόδια αρχή έκθεση σχετικά με το αποτέλεσμα της επαλήθευσης της συμμόρφωσης.

Άρθρο 32

Σύστημα διαχείρισης της κυβερνοασφάλειας

1. Εντός 24 μηνών από την κοινοποίηση από την αρμόδια αρχή του χαρακτηρισμού της ως οντότητας υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6, κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου θεσπίζει σύστημα διαχείρισης της κυβερνοασφάλειας και, στη συνέχεια, το επανεξετάζει ανά τριετία προκειμένου:

α) να καθορίσει το πεδίο εφαρμογής του συστήματος διαχείρισης της κυβερνοασφάλειας λαμβάνοντας υπόψη τις διεπαφές και τις εξαρτήσεις με άλλες οντότητες·

β) να διασφαλίζει ότι όλα τα ανώτερα διοικητικά στελέχη της είναι ενημερωμένα για τις σχετικές νομικές υποχρεώσεις και συμβάλλουν ενεργά στην εφαρμογή του συστήματος διαχείρισης της κυβερνοασφάλειας μέσω έγκαιρων αποφάσεων και άμεσων αντιδράσεων·

γ) να διασφαλίζει ότι οι πόροι που απαιτούνται για το σύστημα διαχείρισης της κυβερνοασφάλειας είναι διαθέσιμοι·

δ) να θεσπίσει πολιτική κυβερνοασφάλειας η οποία τεκμηριώνεται και κοινοποιείται εντός της οντότητας και στα μέρη που επηρεάζονται από τους κινδύνους για την ασφάλεια·

ε) να αναθέτει και να κοινοποιεί αρμοδιότητες για ρόλους που σχετίζονται με την κυβερνοασφάλεια·

στ) να εκτελεί διαχείριση κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας, όπως ορίζεται στο άρθρο 26·

ζ) να καθορίσει και να παρέχει τους πόρους που απαιτούνται για την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση του συστήματος διαχείρισης της κυβερνοασφάλειας, λαμβάνοντας υπόψη την απαραίτητη ικανότητα και επίγνωση των πόρων κυβερνοασφάλειας·

η) να καθορίσει την εσωτερική και εξωτερική επικοινωνία στο πεδίο της κυβερνοασφάλειας·

θ) να δημιουργεί, να επικαιροποιεί και να ελέγχει τεκμηριωμένες πληροφορίες που σχετίζονται με το σύστημα διαχείρισης της κυβερνοασφάλειας·

ι) να αξιολογεί τις επιδόσεις και την αποτελεσματικότητα του συστήματος διαχείρισης της κυβερνοασφάλειας·

ια) να διενεργεί εσωτερικούς ελέγχους σε προγραμματισμένα χρονικά διαστήματα για να διασφαλίζει την αποτελεσματική εφαρμογή και διατήρηση του συστήματος διαχείρισης της κυβερνοασφάλειας·

ιβ) να επανεξετάζει την εφαρμογή του συστήματος διαχείρισης της κυβερνοασφάλειας σε προγραμματισμένα χρονικά διαστήματα· και να ελέγχει και να διορθώνει τυχόν μη συμμόρφωση των πόρων και των δραστηριοτήτων με τις πολιτικές, τις διαδικασίες και τις κατευθυντήριες γραμμές του συστήματος διαχείρισης της κυβερνοασφάλειας.

2. Το πεδίο εφαρμογής του συστήματος διαχείρισης της κυβερνοασφάλειας περιλαμβάνει όλα τα περιουσιακά στοιχεία εντός της περιμέτρου υψηλού ή κρίσιμου αντικτύπου της οντότητας υψηλού ή κρίσιμου αντικτύπου.

3. Οι αρμόδιες αρχές, χωρίς να επιβάλλουν ή να ευνοούν τη χρήση συγκεκριμένου τύπου τεχνολογίας, ενθαρρύνουν τη χρήση ευρωπαϊκών ή διεθνών προτύπων και προδιαγραφών που σχετίζονται με τα συστήματα διαχείρισης και αφορούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

Άρθρο 33

Ελάχιστοι και προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού

1. Εντός 7 μηνών από την υποβολή του πρώτου σχεδίου έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 4, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζουν πρόταση για ελάχιστους και προηγμένους ελέγχους κυβερνοασφάλειας στην αλυσίδα εφοδιασμού, οι οποίοι μετριάζουν τους κινδύνους της αλυσίδας εφοδιασμού που προσδιορίζονται στις εκτιμήσεις κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης, συμπληρώνοντας τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας που έχουν αναπτυχθεί σύμφωνα με το άρθρο 29. Οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού αναπτύσσονται σε συνδυασμό με τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας σύμφωνα με το άρθρο 29. Οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού καλύπτουν ολόκληρο τον κύκλο ζωής όλων των προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ εντός της περιμέτρου υψηλού ή κρίσιμου αντικτύπου μιας οντότητας υψηλού ή κρίσιμου αντικτύπου. Κατά την κατάρτιση της πρότασης για τους ελάχιστους και τους προηγμένους ελέγχους κυβερνοασφάλειας στην αλυσίδα εφοδιασμού, ζητείται η γνώμη της Ομάδας Συνεργασίας NIS.

2. Οι ελάχιστοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού συνίστανται σε ελέγχους για οντότητες υψηλού ή κρίσιμου αντικτύπου οι οποίοι:

α) περιλαμβάνουν συστάσεις για τη σύναψη δημόσιων συμβάσεων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που αναφέρονται σε προδιαγραφές κυβερνοασφάλειας, οι οποίες καλύπτουν τουλάχιστον:

i) τους ελέγχους επαλήθευσης του ιστορικού του προσωπικού του προμηθευτή που συμμετέχει στην αλυσίδα εφοδιασμού και αφορούν τις ευαίσθητες πληροφορίες ή την πρόσβαση στα περιουσιακά στοιχεία υψηλού ή κρίσιμου αντικτύπου της οντότητας. Ο έλεγχος επαλήθευσης ιστορικού μπορεί να περιλαμβάνει επαλήθευση της ταυτότητας και του ιστορικού του προσωπικού ή των αναδόχων μιας οντότητας σύμφωνα με το εθνικό δίκαιο, τις εθνικές διαδικασίες και το συναφές και εφαρμοστέο δίκαιο της Ένωσης, συμπεριλαμβανομένων του κανονισμού (ΕΕ) 2016/679 και της οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([18]). Οι έλεγχοι ιστορικού είναι αναλογικοί και περιορίζονται αυστηρά στα όρια του αναγκαίου. Διενεργούνται με αποκλειστικό σκοπό την αξιολόγηση δυνητικού κινδύνου για την ασφάλεια της οικείας οντότητας. Πρέπει να είναι αναλογικοί προς τις επιχειρηματικές απαιτήσεις, τη διαβάθμιση των πληροφοριών στις οποίες παρέχεται πρόσβαση και τους διαφαινόμενους κινδύνους, και μπορούν να διενεργούνται από την ίδια την οντότητα, από εξωτερική εταιρεία που διενεργεί έλεγχο ή μέσω έγκρισης από κρατικό φορέα·

ii) τις διαδικασίες για τον ασφαλή και ελεγχόμενο σχεδιασμό και την ασφαλή και ελεγχόμενη ανάπτυξη και παραγωγή προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, οι οποίες προωθούν τον σχεδιασμό και την ανάπτυξη προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που περιλαμβάνουν κατάλληλα τεχνικά μέτρα για τη διασφάλιση της κυβερνοασφάλειας·

iii) τον σχεδιασμό συστημάτων δικτύου και πληροφοριών στα οποία οι συσκευές δεν κρίνονται αξιόπιστες ακόμα και όταν βρίσκονται εντός ασφαλούς περιμέτρου, απαιτείται επαλήθευση όλων των αιτημάτων που λαμβάνουν και εφαρμόζεται η αρχή των ελάχιστων προνομίων·

iv) την πρόσβαση του προμηθευτή στα περιουσιακά στοιχεία της οντότητας·

([18]) Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89).

v) τις συμβατικές υποχρεώσεις του προμηθευτή να προστατεύει και να περιορίζει την πρόσβαση στις ευαίσθητες πληροφορίες της οντότητας·

vi) τις βασικές προδιαγραφές δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας για τους υπεργολάβους του προμηθευτή·

vii) την ιχνηλασιμότητα της εφαρμογής των προδιαγραφών κυβερνοασφάλειας από την ανάπτυξη και την παραγωγή έως την παράδοση των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ·

viii) την υποστήριξη για την παροχή ενημερώσεων ασφαλείας καθ' όλη τη διάρκεια ζωής των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ ή των διαδικασιών ΤΠΕ·

ix) το δικαίωμα ελέγχου της κυβερνοασφάλειας στις διαδικασίες σχεδιασμού, ανάπτυξης και παραγωγής του προμηθευτή· και

x) την αξιολόγηση του προφίλ κινδύνου του προμηθευτή·

β) απαιτούν από τις εν λόγω οντότητες να λαμβάνουν υπόψη τις συστάσεις για τη σύναψη δημόσιων συμβάσεων που αναφέρονται στο στοιχείο α) κατά τη σύναψη συμβάσεων με προμηθευτές, συνεργαζόμενους εταίρους και άλλα μέρη στην αλυσίδα εφοδιασμού, οι οποίες καλύπτουν τις συνήθεις παραδόσεις προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ, καθώς και μη ζητηθέντα γεγονότα και περιστάσεις, όπως η καταγγελία και η μεταβίβαση συμβάσεων σε περιπτώσεις αμέλειας του αντισυμβαλλομένου·

γ) απαιτούν από τις εν λόγω οντότητες να λαμβάνουν υπόψη τα αποτελέσματα των σχετικών συντονισμένων εκτιμήσεων κινδύνων για την ασφάλεια σε κρίσιμες αλυσίδες εφοδιασμού, οι οποίες διενεργούνται σύμφωνα με το άρθρο 22 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555·

δ) περιλαμβάνουν κριτήρια για την επιλογή και τη σύναψη συμβάσεων με προμηθευτές οι οποίοι μπορούν να πληρούν τις προδιαγραφές κυβερνοασφάλειας που αναφέρονται στο στοιχείο α) και διαθέτουν επίπεδο κυβερνοασφάλειας κατάλληλο για τους κινδύνους για την κυβερνοασφάλεια του προϊόντος ΤΠΕ, της υπηρεσίας ΤΠΕ ή των διαδικασιών ΤΠΕ που παρέχει ο προμηθευτής·

ε) περιλαμβάνουν κριτήρια για τη διαφοροποίηση των πηγών εφοδιασμού για προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ, και για τη μείωση του κινδύνου εγκλωβισμού σε συγκεκριμένους προμηθευτές·

στ) περιλαμβάνουν κριτήρια για την παρακολούθηση, την επανεξέταση ή τον έλεγχο των προδιαγραφών κυβερνοασφάλειας για τις εσωτερικές επιχειρησιακές διαδικασίες του προμηθευτή καθ' όλη τη διάρκεια του κύκλου ζωής κάθε προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ και διαδικασίας ΤΠΕ σε τακτική βάση.

3. Για τις προδιαγραφές κυβερνοασφάλειας στη σύσταση για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας που αναφέρεται στην παράγραφο 2 στοιχείο α), οι οντότητες υψηλού ή κρίσιμου αντικτύπου χρησιμοποιούν τις αρχές που εφαρμόζονται στη σύναψη δημόσιων συμβάσεων δυνάμει της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([19]), σύμφωνα με το άρθρο 35 παράγραφος 4, ή καθορίζουν τις δικές τους προδιαγραφές με βάση τα αποτελέσματα της εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας.

4. Οι προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού περιλαμβάνουν ελέγχους για την επαλήθευση από τις οντότητες κρίσιμου αντικτύπου, κατά τη διάρκεια της διαδικασίας σύναψης δημόσιων συμβάσεων, ότι τα προϊόντα ΤΠΕ, οι υπηρεσίες ΤΠΕ και οι διαδικασίες ΤΠΕ που θα χρησιμοποιηθούν ως περιουσιακά στοιχεία κρίσιμου αντικτύπου πληρούν τις προδιαγραφές κυβερνοασφάλειας. Το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ ή η διαδικασία ΤΠΕ επαληθεύεται είτε μέσω ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας που αναφέρεται στο άρθρο 31 ή μέσω δραστηριοτήτων επαλήθευσης που επιλέγονται και οργανώνονται από την οντότητα. Το βάθος και η κάλυψη των δραστηριοτήτων επαλήθευσης επαρκούν ώστε να διασφαλίζεται ότι το προϊόν ΤΠΕ, η υπηρεσία ΤΠΕ ή η διαδικασία ΤΠΕ μπορεί να χρησιμοποιηθεί για τον μετριασμό των κινδύνων που έχουν προσδιοριστεί στην εκτίμηση κινδύνων σε επίπεδο οντότητας. Η οντότητα κρίσιμου αντικτύπου τεκμηριώνει τα μέτρα που λαμβάνονται για τη μείωση των κινδύνων που έχουν προσδιοριστεί.

5. Οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού εφαρμόζονται στις δημόσιες συμβάσεις σχετικών προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ. Οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας στην αλυσίδα εφοδιασμού θα εφαρμόζονται στις διαδικασίες σύναψης δημόσιων συμβάσεων στις οντότητες που χαρακτηρίζονται ως οντότητες κρίσιμου ή υψηλού αντικτύπου σύμφωνα με το άρθρο 24, οι οποίες ξεκινούν έξι μήνες μετά την έγκριση ή την επικαιροποίηση των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας που αναφέρονται στο άρθρο 29.

([19]) Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις δημόσιες προμήθειες και την κατάργηση της οδηγίας 2004/18/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 65).

6. Εντός 6 μηνών από την κατάρτιση κάθε περιφερειακής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 21 παράγραφος 2, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, προτείνουν στην αρμόδια αρχή τροποποίηση των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας στην αλυσίδα εφοδιασμού. Η πρόταση θα υποβάλλεται σύμφωνα με το άρθρο 8 παράγραφος 10 και θα λαμβάνει υπόψη τους κινδύνους που προσδιορίστηκαν στην περιφερειακή εκτίμηση κινδύνων.

Άρθρο 34

Πίνακας χαρτογράφησης των ελέγχων κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας με βάση τα πρότυπα

1. Εντός 7 μηνών από την υποβολή του πρώτου σχεδίου έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο Ένωσης σύμφωνα με το άρθρο 19 παράγραφος 4, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και σε διαβούλευση με τον ENISA, καταρτίζουν πρόταση για πίνακα χαρτογράφησης των ελέγχων που ορίζονται στο άρθρο 28 παράγραφος 1 στοιχεία α) και β) με βάση επιλεγμένα ευρωπαϊκά και διεθνή πρότυπα, καθώς και σχετικές τεχνικές προδιαγραφές (στο εξής: πίνακας χαρτογράφησης). Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ τεκμηριώνουν την ισοδυναμία των διαφόρων ελέγχων με τους ελέγχους που ορίζονται στο άρθρο 28 παράγραφος 1 στοιχεία α) και β).

2. Οι αρμόδιες αρχές μπορούν να παρέχουν στο ΕΔΔΣΜ ηλεκτρικής ενέργειας και στον φορέα ΔΣΔ της ΕΕ χαρτογράφηση των ελέγχων που ορίζονται στο άρθρο 28 παράγραφος 1 στοιχεία α) και β) με παραπομπή στα σχετικά εθνικά νομοθετικά ή ρυθμιστικά πλαίσια, συμπεριλαμβανομένων των σχετικών εθνικών προτύπων των κρατών μελών σύμφωνα με το άρθρο 25 της οδηγίας (ΕΕ) 2022/2555. Εάν η αρμόδια αρχή κράτους μέλους παράσχει μια τέτοια χαρτογράφηση, το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ ενσωματώνουν την εν λόγω εθνική χαρτογράφηση στον πίνακα χαρτογράφησης.

3. Εντός 6 μηνών από την κατάρτιση κάθε περιφερειακής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια σύμφωνα με το άρθρο 21 παράγραφος 2, οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ και κατόπιν διαβούλευσης με τον ENISA, προτείνουν τροποποίηση του πίνακα χαρτογράφησης στην αρμόδια αρχή. Η πρόταση θα υποβάλλεται σύμφωνα με το άρθρο 8 παράγραφος 10 και θα λαμβάνει υπόψη τους κινδύνους που προσδιορίστηκαν στην περιφερειακή εκτίμηση κινδύνων.

ΚΕΦΑΛΑΙΟ IV

ΣΥΣΤΑΣΕΙΣ ΓΙΑ ΤΗ ΣΥΝΑΨΗ ΔΗΜΟΣΙΩΝ ΣΥΜΒΑΣΕΩΝ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Άρθρο 35

Συστάσεις για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας

1. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζουν, στο πλαίσιο προγράμματος εργασίας που εκπονείται και επικαιροποιείται κάθε φορά που εγκρίνεται περιφερειακή έκθεση εκτίμησης των κινδύνων για την κυβερνοασφάλεια, δέσμες μη δεσμευτικών συστάσεων για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας, τις οποίες μπορούν να χρησιμοποιούν οντότητες υψηλού ή κρίσιμου αντικτύπου ως βάση για τις δημόσιες συμβάσεις προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ εντός των περιμέτρων υψηλού και κρίσιμου αντικτύπου. Το εν λόγω πρόγραμμα εργασίας περιλαμβάνει τα εξής:

α) περιγραφή και ταξινόμηση των τύπων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που χρησιμοποιούνται από οντότητες υψηλού ή κρίσιμου αντικτύπου εντός της περιμέτρου υψηλού ή κρίσιμου αντικτύπου·

β) κατάλογο των τύπων προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ για τα οποία αναπτύσσεται δέσμη μη δεσμευτικών συστάσεων κυβερνοασφάλειας με βάση τις σχετικές περιφερειακές εκθέσεις εκτίμησης των κινδύνων για την κυβερνοασφάλεια και τις προτεραιότητες των οντοτήτων υψηλού ή κρίσιμου αντικτύπου.

2. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, παρέχει στον ACER περίληψη του εν λόγω προγράμματος εργασίας, εντός 6 μηνών από την έγκριση ή την επικαιροποίηση της περιφερειακής έκθεσης εκτίμησης των κινδύνων για την κυβερνοασφάλεια.

3. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, προσπαθούν να διασφαλίσουν ότι οι μη δεσμευτικές συστάσεις για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας που καταρτίζονται με βάση τη σχετική περιφερειακή εκτίμηση των κινδύνων για την κυβερνοασφάλεια είναι παρόμοιες ή συγκρίσιμες μεταξύ των λειτουργικών περιφερειών του συστήματος. Οι δέσμες συστάσεων για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας καλύπτουν τουλάχιστον τις προδιαγραφές που αναφέρονται στο άρθρο 33 παράγραφος 2 στοιχείο α). Όπου είναι δυνατόν, οι προδιαγραφές επιλέγονται από ευρωπαϊκά και διεθνή πρότυπα.

4. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, διασφαλίζουν ότι οι δέσμες συστάσεων για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας:

α) συμμορφώνονται με τις αρχές που εφαρμόζονται στη σύναψη δημόσιων συμβάσεων σύμφωνα με την οδηγία 2014/24/ΕΕ· και

β) είναι συμβατές με τα πιο πρόσφατα διαθέσιμα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας που αφορούν το προϊόν ΤΠΕ, την υπηρεσία ΤΠΕ ή τη διαδικασία ΤΠΕ, και τα λαμβάνουν υπόψη.

Άρθρο 36

Καθοδήγηση σχετικά με τη χρήση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας για τις δημόσιες συμβάσεις προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ

1. Οι μη δεσμευτικές συστάσεις για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας που καταρτίζονται σύμφωνα με το άρθρο 35 μπορούν να περιλαμβάνουν τομεακή καθοδήγηση σχετικά με τη χρήση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας, στις περιπτώσεις που υπάρχει διαθέσιμο κατάλληλο σχήμα για έναν τύπο προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ που χρησιμοποιείται από οντότητες κρίσιμου αντικτύπου, με την επιφύλαξη του πλαισίου για τη θέσπιση ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας σύμφωνα με το άρθρο 46 του κανονισμού (ΕΕ) 2019/881.

2. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, συνεργάζονται στενά με τον ENISA για την παροχή της τομεακής καθοδήγησης που περιλαμβάνεται σε μη δεσμευτικές συστάσεις για τη σύναψη δημόσιων συμβάσεων στον τομέα της κυβερνοασφάλειας σύμφωνα με την παράγραφο 1.

ΚΕΦΑΛΑΙΟ V

ΡΟΕΣ ΠΛΗΡΟΦΟΡΙΩΝ, ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ

Άρθρο 37

Κανόνες για την ανταλλαγή πληροφοριών

1. Εάν μια αρμόδια αρχή λάβει πληροφορίες σχετικά με κυβερνοεπίθεση που πρέπει να αναφερθεί, η εν λόγω αρμόδια αρχή:

α) αξιολογεί το επίπεδο εμπιστευτικότητας των εν λόγω πληροφοριών και ενημερώνει την οντότητα σχετικά με το αποτέλεσμα της αξιολόγησής της χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 24 ωρών από την παραλαβή των πληροφοριών·

β) προσπαθεί να εντοπίσει οποιαδήποτε άλλη παρόμοια κυβερνοεπίθεση στην Ένωση που έχει αναφερθεί σε άλλες αρμόδιες αρχές, προκειμένου να συσχετίσει τις πληροφορίες τις οποίες έλαβε στο πλαίσιο της κυβερνοεπίθεσης που πρέπει να αναφερθεί με πληροφορίες που έχουν παρασχεθεί στο πλαίσιο άλλων κυβερνοεπιθέσεων και να εμπλουτίσει τις υπάρχουσες πληροφορίες, να ενισχύσει και να συντονίσει τις αντιδράσεις στον τομέα της κυβερνοασφάλειας·

γ) είναι υπεύθυνη για την απάλειψη των στοιχείων που συνιστούν επιχειρηματικό απόρρητο και για την ανωνυμοποίηση των πληροφοριών σύμφωνα με τους σχετικούς εθνικούς και ενωσιακούς κανόνες·

δ) κοινοποιεί τις πληροφορίες στα εθνικά ενιαία σημεία επαφής, στις CSIRT και σε όλες τις αρμόδιες αρχές που έχουν οριστεί σύμφωνα με το άρθρο 4 σε άλλα κράτη μέλη, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 24 ωρών από την παραλαβή των πληροφοριών για κυβερνοεπίθεση που πρέπει να αναφερθεί, και παρέχει επικαιροποιημένες πληροφορίες σε τακτική βάση στις εν λόγω αρχές ή στους εν λόγω φορείς·

ε) διαδίδει τις πληροφορίες σχετικά με την κυβερνοεπίθεση, μετά την ανωνυμοποίηση και την απάλειψη των στοιχείων που συνιστούν επιχειρηματικό απόρρητο σύμφωνα με την παράγραφο 1 στοιχείο γ), σε οντότητες κρίσιμου ή υψηλού αντικτύπου στο οικείο κράτος μέλος, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 24 ωρών από τη λήψη των πληροφοριών σύμφωνα με την παράγραφο 1 στοιχείο α), και παρέχει επικαιροποιημένες πληροφορίες σε τακτική βάση που επιτρέπουν στις οντότητες να οργανώσουν αποτελεσματικά την άμυνά τους·

στ) μπορεί να ζητήσει από την αναφέρουσα οντότητα υψηλού ή κρίσιμου αντικτύπου να διαδώσει περαιτέρω τις πληροφορίες για την κυβερνοεπίθεση που πρέπει να αναφερθεί με ασφαλή τρόπο σε άλλες οντότητες οι οποίες ενδέχεται να επηρεαστούν, με στόχο να υπάρξει επίγνωση της κατάστασης στον τομέα της ηλεκτρικής ενέργειας και να αποτραπεί η επέλευση κινδύνου που ενδέχεται να κλιμακωθεί σε διασυνοριακό περιστατικό κυβερνοασφάλειας στον τομέα της ηλεκτρικής ενέργειας·

ζ) κοινοποιεί στον ENISA συνοπτική έκθεση, μετά την ανωνυμοποίηση και την απάλειψη των στοιχείων που συνιστούν επιχειρηματικό απόρρητο, με τις πληροφορίες σχετικά με την κυβερνοεπίθεση.

2. Εάν μια CSIRT λάβει γνώση μη διορθωμένης ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης, οφείλει:

α) να την κοινοποιήσει στον ENISA μέσω κατάλληλου ασφαλούς διαύλου ανταλλαγής πληροφοριών χωρίς καθυστέρηση, εκτός εάν ορίζεται διαφορετικά σε άλλες διατάξεις του δικαίου της Ένωσης·

β) να υποστηρίξει την ενδιαφερόμενη οντότητα ώστε να λάβει από τον κατασκευαστή ή τον πάροχο αποτελεσματική, συντονισμένη και ταχεία διαχείριση της μη διορθωμένης ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης ή αποτελεσματικά και αποδοτικά μέτρα μετριασμού·

γ) να κοινοποιήσει τις διαθέσιμες πληροφορίες στον πωλητή και να ζητήσει από τον κατασκευαστή ή τον πάροχο, όπου είναι δυνατόν, να καταρτίσει κατάλογο των CSIRT στα κράτη μέλη τις οποίες αφορά η μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και οι οποίες ενημερώνονται σχετικά·

δ) να κοινοποιήσει τις διαθέσιμες πληροφορίες στις CSIRT που προσδιορίζονται σύμφωνα με το προηγούμενο στοιχείο, με βάση την αρχή της ανάγκης για γνώση·

ε) να κοινοποιήσει, όπου υπάρχουν, στρατηγικές και μέτρα μετριασμού για την αναφερθείσα μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης.

3. Εάν μια αρμόδια αρχή λάβει γνώση μη διορθωμένης ευπάθειας που αποτελεί αντικείμενο ενεργού εκμετάλλευσης:

α) κοινοποιεί, στην περίπτωση που υπάρχουν, στρατηγικές και μέτρα μετριασμού για την αναφερθείσα μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης, σε συντονισμό με τις CSIRT στο οικείο κράτος μέλος·

β) κοινοποιεί τις πληροφορίες σε CSIRT στο κράτος μέλος στο οποίο έχει αναφερθεί η μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης.

4. Εάν η αρμόδια αρχή λάβει γνώση μη διορθωμένης ευπάθειας χωρίς να υπάρχουν στοιχεία που να αποδεικνύουν ότι αποτελεί αντικείμενο ενεργού εκμετάλλευσης, συντονίζεται χωρίς αδικαιολόγητη καθυστέρηση με τη CSIRT για τους σκοπούς της συντονισμένης γνωστοποίησης ευπαθειών, όπως ορίζεται στο άρθρο 12 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555.

5. Εάν μια CSIRT λάβει πληροφορίες που σχετίζονται με κυβερνοαπειλές από μία ή περισσότερες οντότητες υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 38 παράγραφος 6, διαδίδει τις εν λόγω πληροφορίες ή κάθε άλλη πληροφορία που είναι σημαντική για την πρόληψη, την ανίχνευση, την αντιμετώπιση ή τον μετριασμό του σχετικού κινδύνου στις οντότητες κρίσιμου ή υψηλού αντικτύπου στο οικείο κράτος μέλος και, κατά περίπτωση, σε όλες τις ενδιαφερόμενες CSIRT και στο οικείο εθνικό ενιαίο σημείο επαφής, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο τέσσερις ώρες μετά τη λήψη των πληροφοριών.

6. Εάν μια αρμόδια αρχή λάβει γνώση πληροφοριών σχετικά με κυβερνοαπειλές από μία ή περισσότερες οντότητες υψηλού ή κρίσιμου αντικτύπου, διαβιβάζει τις πληροφορίες αυτές στην CSIRT για τους σκοπούς της παραγράφου 5.

7. Οι αρμόδιες αρχές μπορούν να αναθέτουν πλήρως ή εν μέρει τις αρμοδιότητες που προβλέπονται στις παραγράφους 3 και 4 σχετικά με μία ή περισσότερες οντότητες υψηλού ή κρίσιμου αντικτύπου που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη σε άλλη αρμόδια αρχή σε ένα από τα εν λόγω κράτη μέλη, κατόπιν συμφωνίας μεταξύ των ενδιαφερόμενων αρμόδιων αρχών.

8. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, αναπτύσσουν μεθοδολογία κλίμακας ταξινόμησης κυβερνοεπιθέσεων έως τις 13 Ιουνίου 2025. Οι ΔΣΜ, με τη συνδρομή του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ, μπορούν να ζητήσουν από τις αρμόδιες αρχές να λάβουν τη γνώμη του ENISA και των οικείων αρμόδιων αρχών που είναι υπεύθυνες για την κυβερνοασφάλεια, προκειμένου να λάβουν βοήθεια για την ανάπτυξη της εν λόγω κλίμακας ταξινόμησης. Η μεθοδολογία καθορίζει την ταξινόμηση της σοβαρότητας μιας κυβερνοεπίθεσης σύμφωνα με 5 επίπεδα, εκ των οποίων τα δύο υψηλότερα είναι το «υψηλό» και το «κρίσιμο». Η ταξινόμηση βασίζεται στην αξιολόγηση των ακόλουθων παραμέτρων:

α) του δυνητικού αντικτύπου, λαμβανομένων υπόψη των περιουσιακών στοιχείων και των περιμέτρων που εκτίθενται, όπως προσδιορίζονται σύμφωνα με το άρθρο 26 παράγραφος 4 στοιχείο γ)· και

β) της σοβαρότητας της κυβερνοεπίθεσης.

9. Έως τις 13 Ιουνίου 2026 το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, εκπονεί μελέτη σκοπιμότητας για να αξιολογήσει τη δυνατότητα και το οικονομικό κόστος που απαιτείται για την ανάπτυξη κοινού εργαλείου που θα παρέχει σε όλες τις οντότητες τη δυνατότητα να ανταλλάσσουν πληροφορίες με τις αρμόδιες εθνικές αρχές.

10. Η μελέτη σκοπιμότητας εξετάζει τη δυνατότητα που έχει ένα τέτοιο κοινό εργαλείο:

α) να υποστηρίζει οντότητες κρίσιμου ή υψηλού αντικτύπου με την παροχή σχετικών πληροφοριών που αφορούν την ασφάλεια για δραστηριότητες διασυνοριακών ροών ηλεκτρικής ενέργειας, όπως αναφορά κυβερνοεπιθέσεων σε σχεδόν πραγματικό χρόνο, έγκαιρες προειδοποιήσεις που σχετίζονται με ζητήματα κυβερνοασφάλειας και μη γνωστοποιημένες ευπάθειες του εξοπλισμού που χρησιμοποιείται στο σύστημα ηλεκτρικής ενέργειας·

β) να διατηρείται σε κατάλληλο και άκρως αξιόπιστο περιβάλλον·

γ) να καθιστά δυνατή τη συλλογή δεδομένων από οντότητες κρίσιμου ή υψηλού αντικτύπου και να διευκολύνει την απάλειψη εμπιστευτικών πληροφοριών και την ανωνυμοποίηση των δεδομένων, καθώς και την άμεση διάδοσή τους σε οντότητες κρίσιμου ή υψηλού αντικτύπου.

11. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ:

α) ζητεί τη γνώμη του ENISA και της Ομάδας Συνεργασίας NIS, των εθνικών ενιαίων σημείων επαφής και των εκπροσώπων των κύριων ενδιαφερόμενων μερών κατά την αξιολόγηση της σκοπιμότητας·

β) παρουσιάζει τα αποτελέσματα της μελέτης σκοπιμότητας στον ACER και στην Ομάδα Συνεργασίας NIS.

12. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, μπορεί να αναλύει και να διευκολύνει τις πρωτοβουλίες που προτείνονται από οντότητες κρίσιμου ή υψηλού αντικτύπου για την αξιολόγηση και τη δοκιμή τέτοιων εργαλείων ανταλλαγής πληροφοριών.

Άρθρο 38

Ρόλος των οντοτήτων υψηλού ή κρίσιμου αντικτύπου όσον αφορά την ανταλλαγή πληροφοριών

1. Κάθε οντότητα υψηλού ή κρίσιμου αντικτύπου:

α) καθορίζει, για όλα τα περιουσιακά στοιχεία εντός της οικείας περιμέτρου κυβερνοασφάλειας που προσδιορίζεται σύμφωνα με το άρθρο 26 παράγραφος 4 στοιχείο γ), τουλάχιστον τις ικανότητες του κέντρου επιχειρήσεων κυβερνοασφάλειας (CSOC):

i) να διασφαλίζει ότι τα σχετικά συστήματα και εφαρμογές δικτύου και πληροφοριών παρέχουν αρχεία καταγραφής ασφάλειας για την παρακολούθηση της ασφάλειας, ώστε να καθίσταται δυνατή η ανίχνευση ανωμαλιών και να συλλέγονται πληροφορίες σχετικά με κυβερνοεπιθέσεις·

ii) να παρακολουθεί την ασφάλεια, μεταξύ άλλων ανιχνεύοντας εισβολές και αξιολογώντας τις ευπάθειες των συστημάτων δικτύου και πληροφοριών·

iii) να αναλύει και, εάν είναι αναγκαίο, να λαμβάνει όλα τα μέτρα που απαιτούνται στο πλαίσιο της ευθύνης και των ικανοτήτων του για να προστατεύει την οντότητα·

iv) να συμμετέχει στη συλλογή και ανταλλαγή πληροφοριών που περιγράφονται στο παρόν άρθρο·

β) έχει το δικαίωμα να προμηθεύεται το σύνολο ή μέρος αυτών των ικανοτήτων σύμφωνα με το στοιχείο α) μέσω παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας. Οι οντότητες κρίσιμου και υψηλού αντικτύπου παραμένουν υπεύθυνες για τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας και εποπτεύουν τις προσπάθειές τους·

γ) ορίζει ενιαίο σημείο επαφής σε επίπεδο οντότητας για τους σκοπούς της ανταλλαγής πληροφοριών.

2. Ο ENISA μπορεί να εκδίδει μη δεσμευτική καθοδήγηση σχετικά με τη δημιουργία των εν λόγω ικανοτήτων ή την εξωτερική ανάθεση της υπηρεσίας σε παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, στο πλαίσιο των καθηκόντων που ορίζονται στο άρθρο 6 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881.

3. Κάθε οντότητα κρίσιμου ή υψηλού αντικτύπου κοινοποιεί στις οικείες CSIRT και στην οικεία αρμόδια αρχή τις σχετικές πληροφορίες που αφορούν κυβερνοεπίθεση που πρέπει να αναφερθεί, χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός τεσσάρων ωρών από τη στιγμή που αντιλαμβάνεται ότι το περιστατικό πρέπει να αναφερθεί.

4. Οι πληροφορίες σχετικά με κυβερνοεπίθεση θεωρείται ότι πρέπει να αναφερθούν όταν η κυβερνοεπίθεση αξιολογείται από την επηρεαζόμενη οντότητα και η κρισιμότητά της εντάσσεται στις κατηγορίες «υψηλή» ή «κρίσιμη» με βάση τη μεθοδολογία της κλίμακας ταξινόμησης κυβερνοεπιθέσεων σύμφωνα με το άρθρο 37 παράγραφος 8. Το ενιαίο σημείο επαφής σε επίπεδο οντότητας που ορίζεται σύμφωνα με την παράγραφο 1 στοιχείο γ) κοινοποιεί την ταξινόμηση του περιστατικού.

5. Όταν οντότητες κρίσιμου και υψηλού αντικτύπου κοινοποιούν σε μια CSIRT σχετικές πληροφορίες που αφορούν μη διορθωμένες ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης, η CSIRT μπορεί να διαβιβάζει τις πληροφορίες αυτές στην οικεία αρμόδια αρχή. Λαμβανομένου υπόψη του βαθμού ευαισθησίας των κοινοποιούμενων πληροφοριών, η CSIRT μπορεί να αρνηθεί να διαβιβάσει τις πληροφορίες ή να καθυστερήσει τη διαβίβασή τους για αιτιολογημένους λόγους που σχετίζονται με την κυβερνοασφάλεια.

6. Κάθε οντότητα κρίσιμου ή υψηλού αντικτύπου παρέχει στις οικείες CSIRT, χωρίς αδικαιολόγητη καθυστέρηση, κάθε πληροφορία η οποία σχετίζεται με κυβερνοαπειλή που πρέπει να αναφερθεί και που ενδέχεται να έχει διασυνοριακές επιπτώσεις. Οι πληροφορίες σχετικά με κυβερνοαπειλή θεωρείται ότι πρέπει να αναφέρονται όταν πληρούται τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) παρέχουν σχετικές πληροφορίες για άλλη οντότητα κρίσιμου ή υψηλού αντικτύπου, για την πρόληψη, την ανίχνευση, την αντιμετώπιση ή τον μετριασμό του αντικτύπου του κινδύνου·

β) οι προσδιοριζόμενες τεχνικές, τακτικές και διαδικασίες που χρησιμοποιούνται στο πλαίσιο επίθεσης οδηγούν σε πληροφορίες όπως παραβίαση διευθύνσεων ομοιόμορφου εντοπιστή πόρου (URL) ή πρωτοκόλλου διαδικτύου (IP), κατακερματισμοί ή οποιοδήποτε άλλο χαρακτηριστικό που είναι χρήσιμο για την ένταξη της επίθεσης σε πλαίσιο και τη συσχέτισή της·

γ) μια κυβερνοαπειλή μπορεί να αξιολογηθεί περαιτέρω και να ενταχθεί σε πλαίσιο με πρόσθετες πληροφορίες που παρέχονται από παρόχους υπηρεσιών ή τρίτα μέρη που δεν υπόκεινται στον παρόντα κανονισμό.

7. Κάθε οντότητα κρίσιμου ή υψηλού αντικτύπου, κατά την ανταλλαγή πληροφοριών σύμφωνα με το παρόν άρθρο, προσδιορίζει τα ακόλουθα:

α) ότι οι πληροφορίες υποβάλλονται σύμφωνα με τον παρόντα κανονισμό·

β) αν οι πληροφορίες αφορούν:

i) κυβερνοεπίθεση που πρέπει να αναφερθεί, όπως αναφέρεται στην παράγραφο 3·

ii) μη διορθωμένη ευπάθεια που αποτελεί αντικείμενο ενεργού εκμετάλλευσης και δεν είναι δημόσια γνωστή, όπως αναφέρεται στην παράγραφο 4·

iii) κυβερνοαπειλή που πρέπει να αναφερθεί, όπως αναφέρεται στην παράγραφο 5·

γ) στην περίπτωση κυβερνοεπίθεσης που πρέπει να αναφερθεί, το επίπεδο της κυβερνοεπίθεσης σύμφωνα με τη μεθοδολογία της κλίμακας ταξινόμησης κυβερνοεπιθέσεων που αναφέρεται στο άρθρο 37 παράγραφος 8 και τις πληροφορίες που οδηγούν στην ταξινόμηση αυτή, συμπεριλαμβανομένης τουλάχιστον της κρισιμότητας της κυβερνοεπίθεσης.

8. Όταν μια οντότητα κρίσιμου ή υψηλού αντικτύπου κοινοποιεί σημαντικό περιστατικό σύμφωνα με το άρθρο 23 της οδηγίας (ΕΕ) 2022/2555 και η αναφορά του περιστατικού βάσει του εν λόγω άρθρου περιέχει σχετικές πληροφορίες, όπως απαιτείται βάσει της παραγράφου 3 του παρόντος άρθρου, η αναφορά της οντότητας βάσει του άρθρου 23 παράγραφος 1 της εν λόγω οδηγίας συνιστά αναφορά πληροφοριών σύμφωνα με την παράγραφο 3 του παρόντος άρθρου.

9. Κάθε οντότητα κρίσιμου ή υψηλού αντικτύπου υποβάλλει έκθεση στην οικεία αρμόδια αρχή ή στην CSIRT προσδιορίζοντας με σαφήνεια συγκεκριμένες πληροφορίες που κοινοποιούνται μόνο στην αρμόδια αρχή ή στην CSIRT σε περιπτώσεις στις οποίες η ανταλλαγή πληροφοριών θα μπορούσε να αποτελέσει πηγή κυβερνοεπίθεσης. Κάθε οντότητα κρίσιμου ή υψηλού αντικτύπου έχει το δικαίωμα να παρέχει μη εμπιστευτική έκδοση των πληροφοριών στην αρμόδια CSIRT.

Άρθρο 39

Ανίχνευση κυβερνοεπιθέσεων και χειρισμός σχετικών πληροφοριών

1. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου αναπτύσσουν τις αναγκαίες ικανότητες για τον χειρισμό των κυβερνοεπιθέσεων που ανιχνεύονται με την αναγκαία υποστήριξη της σχετικής αρμόδιας αρχής, του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου μπορεί να υποστηρίζονται από την CSIRT που ορίζεται στο οικείο αντίστοιχο κράτος μέλος στο πλαίσιο των καθηκόντων που ανατίθενται στις CSIRT βάσει του άρθρου 11 παράγραφος 5 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου εφαρμόζουν αποτελεσματικές διαδικασίες για τον εντοπισμό, την ταξινόμηση και την αντιμετώπιση κυβερνοεπιθέσεων που θα επηρεάσουν ή ενδέχεται να επηρεάσουν τις διασυνοριακές ροές ηλεκτρικής ενέργειας, προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις τους.

2. Εάν μια κυβερνοεπίθεση έχει αντίκτυπο στις διασυνοριακές ροές ηλεκτρικής ενέργειας, τα ενιαία σημεία επαφής σε επίπεδο οντότητας των επηρεαζόμενων οντοτήτων κρίσιμου και υψηλού αντικτύπου συνεργάζονται για την ανταλλαγή πληροφοριών μεταξύ τους, υπό τον συντονισμό της αρμόδιας αρχής του κράτους μέλους στο οποίο αναφέρθηκε για πρώτη φορά η κυβερνοεπίθεση.

3. Οι οντότητες κρίσιμου και υψηλού αντικτύπου:

α) διασφαλίζουν ότι το οικείο ενιαίο σημείο επαφής σε επίπεδο οντότητας έχει πρόσβαση, βάσει της ανάγκης για γνώση, στις πληροφορίες που λαμβάνουν από το εθνικό ενιαίο σημείο επαφής μέσω της αρμόδιας αρχής τους·

β) εκτός εάν έχει ήδη πραγματοποιηθεί σύμφωνα με το άρθρο 3 παράγραφος 4 της οδηγίας (ΕΕ) 2022/2555, κοινοποιούν στην αρμόδια αρχή του κράτους μέλους στο οποίο είναι εγκατεστημένες και στο εθνικό ενιαίο σημείο επαφής κατάλογο των οικείων ενιαίων σημείων επαφής για την κυβερνοασφάλεια σε επίπεδο οντότητας:

   i) από τα οποία η εν λόγω αρμόδια αρχή και το εν λόγω εθνικό ενιαίο σημείο επαφής μπορεί να αναμένουν ότι θα λάβουν πληροφορίες σχετικά με κυβερνοεπιθέσεις που πρέπει να αναφερθούν·

   ii) στα οποία οι αρμόδιες αρχές και τα εθνικά ενιαία σημεία επαφής ενδέχεται να πρέπει να παρέχουν πληροφορίες·

γ) θεσπίζουν διαδικασίες διαχείρισης κυβερνοεπιθέσεων, συμπεριλαμβανομένων ρόλων και αρμοδιοτήτων, καθηκόντων και αντιδράσεων με βάση την παρατηρήσιμη εξέλιξη της κυβερνοεπίθεσης εντός των περιμέτρων κρίσιμου και υψηλού αντικτύπου·

δ) υποβάλλουν σε δοκιμή τις συνολικές διαδικασίες διαχείρισης κυβερνοεπιθέσεων, τουλάχιστον σε ετήσια βάση, πραγματοποιώντας δοκιμή τουλάχιστον ενός σεναρίου που επηρεάζει άμεσα ή έμμεσα τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Η εν λόγω ετήσια δοκιμή μπορεί να διενεργείται από οντότητες κρίσιμου ή υψηλού αντικτύπου κατά τη διάρκεια των τακτικών ασκήσεων που αναφέρονται στο άρθρο 43. Κάθε δραστηριότητα άμεσης αντιμετώπισης κυβερνοεπιθέσεων με συνέπεια που ταξινομείται τουλάχιστον στην κατηγορία 2, σύμφωνα με τη μεθοδολογία της κλίμακας ταξινόμησης κυβερνοεπιθέσεων που αναφέρεται στο άρθρο 37 παράγραφος 8, της οποίας τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας, μπορεί να χρησιμεύσει ως ετήσια δοκιμή του σχεδίου αντιμετώπισης κυβερνοεπιθέσεων.

4. Τα καθήκοντα που αναφέρονται στην παράγραφο 1 μπορούν να ανατίθενται από τα κράτη μέλη και στα περιφερειακά συντονιστικά κέντρα σύμφωνα με το άρθρο 37 παράγραφος 2 του κανονισμού (ΕΕ) 2019/943.

Άρθρο 40

Διαχείριση κρίσεων

1. Όταν η αρμόδια αρχή διαπιστώνει ότι μια κρίση ηλεκτρικής ενέργειας σχετίζεται με κυβερνοεπίθεση που έχει αντίκτυπο σε περισσότερα από ένα κράτη μέλη, οι αρμόδιες αρχές των επηρεαζόμενων κρατών μελών, οι ΕΑΑ κυβερνοασφάλειας, οι ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων και οι αρχές διαχείρισης κυβερνοκρίσεων NIS των επηρεαζόμενων κρατών μελών συγκροτούν από κοινού ad hoc ομάδα συντονισμού της διασυνοριακής κρίσης.

2. Η ad hoc ομάδα συντονισμού της διασυνοριακής κρίσης:

α) συντονίζει την αποδοτική ανάκτηση και περαιτέρω διάδοση όλων των σχετικών πληροφοριών κυβερνοασφάλειας στις οντότητες που συμμετέχουν στη διαδικασία διαχείρισης κρίσεων·

β) οργανώνει την επικοινωνία μεταξύ όλων των οντοτήτων που επηρεάζονται από την κρίση και των αρμόδιων αρχών, προκειμένου να μειωθούν οι αλληλεπικαλύψεις και να αυξηθεί η αποδοτικότητα των αναλύσεων και των τεχνικών μέτρων για την αντιμετώπιση των ταυτόχρονων κρίσεων ηλεκτρικής ενέργειας των οποίων τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας·

γ) παρέχει, σε συνεργασία με τις αρμόδιες CSIRT, την απαιτούμενη εμπειρογνωσία, συμπεριλαμβανομένων επιχειρησιακών συμβουλών σχετικά με την εφαρμογή πιθανών μέτρων μετριασμού στις οντότητες που επηρεάζονται από το περιστατικό·

δ) κοινοποιεί και παρέχει τακτικές επικαιροποιήσεις σχετικά με την κατάσταση του περιστατικού στην Επιτροπή και στη Συντονιστική Ομάδα στον τομέα του Ηλεκτρισμού, σύμφωνα με τις αρχές προστασίας που ορίζονται στο άρθρο 46·

ε) ζητεί συμβουλές από αρμόδιες αρχές, οργανισμούς ή οντότητες που ενδέχεται να είναι χρήσιμες για τον μετριασμό της κρίσης ηλεκτρικής ενέργειας.

3. Όταν η κυβερνοεπίθεση χαρακτηρίζεται ή αναμένεται να χαρακτηριστεί ως κυβερνοπεριστατικό μεγάλης κλίμακας, η ad hoc ομάδα συντονισμού της διασυνοριακής κρίσης ενημερώνει αμέσως τις εθνικές αρχές διαχείρισης κυβερνοκρίσεων σύμφωνα με το άρθρο 9 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555 στα κράτη μέλη που επηρεάζονται από το περιστατικό, καθώς και την Επιτροπή και το EU-CyCLONe. Στην περίπτωση αυτήν, η ad hoc ομάδα συντονισμού της διασυνοριακής κρίσης στηρίζει το EU-CyCLONe όσον αφορά τις τομεακές ιδιαιτερότητες.

4. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου αναπτύσσουν και έχουν στη διάθεσή τους ικανότητες, εσωτερικές κατευθυντήριες γραμμές, σχέδια ετοιμότητας και προσωπικό για να συμμετέχουν στην ανίχνευση και στον μετριασμό της διασυνοριακής κρίσης. Η οντότητα κρίσιμου ή υψηλού αντικτύπου που επηρεάζεται από ταυτόχρονη κρίση ηλεκτρικής ενέργειας διερευνά τη βασική αιτία της εν λόγω κρίσης σε συνεργασία με την οικεία αρμόδια αρχή για να διαπιστώσει τον βαθμό στον οποίο η κρίση σχετίζεται με κυβερνοεπίθεση.

5. Τα καθήκοντα που αναφέρονται στην παράγραφο 4 μπορούν να ανατίθενται από τα κράτη μέλη και στα περιφερειακά συντονιστικά κέντρα σύμφωνα με το άρθρο 37 παράγραφος 2 του κανονισμού (ΕΕ) 2019/943.

Άρθρο 41

Σχέδια διαχείρισης και αντιμετώπισης κρίσεων κυβερνοασφάλειας

1. Εντός 24 μηνών από την κοινοποίηση στον ACER της έκθεσης εκτίμησης των κινδύνων σε επίπεδο Ένωσης, ο ACER, σε στενή συνεργασία με τον ENISA, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, τον φορέα ΔΣΔ της ΕΕ, τις ΕΑΑ κυβερνοασφάλειας, τις αρμόδιες αρχές, τις ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων, τις εθνικές ρυθμιστικές αρχές και τις εθνικές αρχές διαχείρισης κυβερνοκρίσεων NIS, καταρτίζει σχέδιο διαχείρισης και αντιμετώπισης κρίσεων κυβερνοασφάλειας σε επίπεδο Ένωσης για τον τομέα της ηλεκτρικής ενέργειας.

2. Εντός 12 μηνών από την κατάρτιση από τον ACER του σχεδίου διαχείρισης και αντιμετώπισης κρίσεων κυβερνοασφάλειας σε επίπεδο Ένωσης για τον τομέα της ηλεκτρικής ενέργειας σύμφωνα με την παράγραφο 1, κάθε αρμόδια αρχή καταρτίζει εθνικό σχέδιο διαχείρισης και αντιμετώπισης κρίσεων κυβερνοασφάλειας για τις διασυνοριακές ροές ηλεκτρικής ενέργειας, λαμβάνοντας υπόψη το σχέδιο διαχείρισης κρίσεων κυβερνοασφάλειας σε επίπεδο Ένωσης και το εθνικό σχέδιο ετοιμότητας αντιμετώπισης κινδύνων που θεσπίζεται σύμφωνα με το άρθρο 10 του κανονισμού (ΕΕ) 2019/941. Το εν λόγω σχέδιο συνάδει με το σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 9 παράγραφος 4 της οδηγίας (ΕΕ) 2022/2555. Η αρμόδια αρχή συντονίζεται με τις οντότητες κρίσιμου ή υψηλού αντικτύπου και με την ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων στο κράτος μέλος της.

3. Το εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας που απαιτείται σύμφωνα με το άρθρο 9 παράγραφος 4 της οδηγίας (ΕΕ) 2022/2555 θεωρείται εθνικό σχέδιο διαχείρισης κρίσεων κυβερνοασφάλειας δυνάμει του παρόντος άρθρου, εάν περιλαμβάνει διατάξεις για τη διαχείριση και την αντιμετώπιση κρίσεων που αφορούν τις διασυνοριακές ροές ηλεκτρικής ενέργειας.

4. Τα καθήκοντα που αναφέρονται στις παραγράφους 1 και 2 μπορούν να ανατίθενται από τα κράτη μέλη και στα περιφερειακά συντονιστικά κέντρα σύμφωνα με το άρθρο 37 παράγραφος 2 του κανονισμού (ΕΕ) 2019/943.

5. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου διασφαλίζουν ότι οι οικείες διαδικασίες διαχείρισης κρίσεων που σχετίζονται με την κυβερνοασφάλεια:

α) διαθέτουν συμβατές διαδικασίες χειρισμού διασυνοριακών κυβερνοπεριστατικών, όπως ορίζεται στο άρθρο 6 παράγραφος 8 της οδηγίας (ΕΕ) 2022/2555, οι οποίες ενσωματώνονται επίσημα στα οικεία σχέδια διαχείρισης κρίσεων·

β) αποτελούν μέρος των γενικών δραστηριοτήτων διαχείρισης κρίσεων.

6. Εντός 12 μηνών από την κοινοποίηση των οντοτήτων υψηλού ή κρίσιμου αντικτύπου σύμφωνα με το άρθρο 24 παράγραφος 6 και, στη συνέχεια, ανά τριετία, οι οντότητες κρίσιμου ή υψηλού αντικτύπου καταρτίζουν σχέδιο διαχείρισης κρίσεων σε επίπεδο οντότητας για κρίσεις που σχετίζονται με την κυβερνοασφάλεια, το οποίο περιλαμβάνεται στα γενικά τους σχέδια διαχείρισης κρίσεων. Το σχέδιο αυτό περιλαμβάνει τουλάχιστον τα ακόλουθα:

α) κανόνες κήρυξης της κρίσης, όπως ορίζεται στο άρθρο 14 παράγραφοι 2 και 3 του κανονισμού (ΕΕ) 2019/941·

β) σαφείς ρόλους και αρμοδιότητες για τη διαχείριση κρίσεων, συμπεριλαμβανομένου του ρόλου άλλων σχετικών οντοτήτων κρίσιμου ή υψηλού αντικτύπου·

γ) επικαιροποιημένα στοιχεία επικοινωνίας, καθώς και κανόνες για την επικοινωνία και την ανταλλαγή πληροφοριών κατά τη διάρκεια κατάστασης κρίσης, συμπεριλαμβανομένης της σύνδεσης με τις CSIRT.

7. Τα μέτρα για τη διαχείριση κρίσεων σύμφωνα με το άρθρο 21 παράγραφος 2 στοιχείο γ) της οδηγίας (ΕΕ) 2022/2555 θεωρούνται σχέδιο διαχείρισης κρίσεων σε επίπεδο οντότητας για τον τομέα της ηλεκτρικής ενέργειας δυνάμει του παρόντος άρθρου, εάν καλύπτουν όλες τις απαιτήσεις που αναφέρονται στην παράγραφο 6.

8. Τα σχέδια διαχείρισης κρίσεων υποβάλλονται σε δοκιμή κατά τη διάρκεια των ασκήσεων κυβερνοασφάλειας που αναφέρονται στα άρθρα 43, 44 και 45.

9. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου περιλαμβάνουν τα οικεία σχέδια διαχείρισης κρίσεων σε επίπεδο οντότητας στα οικεία σχέδια επιχειρηματικής συνέχειας για τις διαδικασίες κρίσιμου και υψηλού αντικτύπου. Τα σχέδια διαχείρισης κρίσεων σε επίπεδο οντότητας περιλαμβάνουν:

α) διαδικασίες ανάλογα με τη διαθεσιμότητα, την ακεραιότητα και την αξιοπιστία των υπηρεσιών ΤΠ·

β) όλες τις τοποθεσίες διασφάλισης της επιχειρηματικής συνέχειας, συμπεριλαμβανομένων των τοποθεσιών υλισμικού και λογισμικού·

γ) όλους τους εσωτερικούς ρόλους και αρμοδιότητες που συνδέονται με τις διαδικασίες επιχειρηματικής συνέχειας.

10. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου επικαιροποιούν τα οικεία σχέδια διαχείρισης κρίσεων σε επίπεδο οντότητας τουλάχιστον ανά τριετία και όποτε είναι αναγκαίο.

11. Ο ACER επικαιροποιεί το σχέδιο διαχείρισης και αντιμετώπισης κρίσεων κυβερνοασφάλειας σε επίπεδο Ένωσης για τον τομέα της ηλεκτρικής ενέργειας, το οποίο καταρτίζεται σύμφωνα με την παράγραφο 1, τουλάχιστον ανά τριετία και όποτε είναι αναγκαίο.

12. Κάθε αρμόδια αρχή επικαιροποιεί το εθνικό σχέδιο διαχείρισης και αντιμετώπισης κρίσεων στον τομέα της κυβερνοασφάλειας για τις διασυνοριακές ροές ηλεκτρικής ενέργειας, το οποίο καταρτίζεται σύμφωνα με την παράγραφο 2, τουλάχιστον ανά τριετία και όποτε απαιτείται.

13. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου υποβάλλουν σε δοκιμή τα οικεία σχέδια επιχειρηματικής συνέχειας τουλάχιστον μία φορά ανά τριετία ή μετά από σημαντικές αλλαγές σε διαδικασία κρίσιμου αντικτύπου. Το αποτέλεσμα των δοκιμών του σχεδίου επιχειρηματικής συνέχειας τεκμηριώνεται. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου μπορούν να περιλαμβάνουν τη δοκιμή του οικείου σχεδίου επιχειρηματικής συνέχειας στις ασκήσεις κυβερνοασφάλειας.

14. Οι οντότητες κρίσιμου ή υψηλού αντικτύπου επικαιροποιούν το οικείο σχέδιο επιχειρηματικής συνέχειας όποτε είναι αναγκαίο και τουλάχιστον μία φορά ανά τριετία, λαμβάνοντας υπόψη το αποτέλεσμα της δοκιμής.

15. Εάν κατά τη δοκιμή διαπιστωθούν ελλείψεις στο σχέδιο επιχειρηματικής συνέχειας, η οντότητα κρίσιμου ή υψηλού αντικτύπου διορθώνει τις εν λόγω ελλείψεις εντός 180 ημερολογιακών ημερών από τη δοκιμή και διενεργεί νέα δοκιμή για να παράσχει στοιχεία που αποδεικνύουν ότι τα διορθωτικά μέτρα είναι αποτελεσματικά.

16. Όταν μια οντότητα κρίσιμου ή υψηλού αντικτύπου δεν μπορεί να διορθώσει τις ελλείψεις εντός 180 ημερολογιακών ημερών, περιλαμβάνει τους σχετικούς λόγους στην έκθεση που πρέπει να υποβληθεί στην οικεία αρμόδια αρχή σύμφωνα με το άρθρο 27.

Άρθρο 42

Ικανότητες έγκαιρης προειδοποίησης για την κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας

1. Οι αρμόδιες αρχές συνεργάζονται με τον ENISA για την ανάπτυξη ικανοτήτων έγκαιρης προειδοποίησης για την κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας (στο εξής: ECEAC) στο πλαίσιο της συνδρομής προς τα κράτη μέλη σύμφωνα με το άρθρο 6 παράγραφος 2 και το άρθρο 7 του κανονισμού (ΕΕ) 2019/881.

2. Κατά την εκτέλεση των καθηκόντων που αναφέρονται στο άρθρο 7 παράγραφος 7 του κανονισμού (ΕΕ) 2019/881, οι ECEAC παρέχουν στον ENISA τη δυνατότητα:

α) να συλλέγει πληροφορίες που κοινοποιούνται σε εθελούσια βάση από:

i) CSIRT, αρμόδιες αρχές·

ii) τις οντότητες που αναφέρονται στο άρθρο 2 του παρόντος κανονισμού·

iii) κάθε άλλη οντότητα που επιθυμεί να κοινοποιήσει σχετικές πληροφορίες σε εθελούσια βάση·

β) να αξιολογεί και να ταξινομεί τις συλλεγόμενες πληροφορίες·

γ) να αξιολογεί τις πληροφορίες στις οποίες έχει πρόσβαση ο ENISA για τον προσδιορισμό των συνθηκών κυβερνοκινδύνου και των σχετικών δεικτών για πτυχές στις διασυνοριακές ροές ηλεκτρικής ενέργειας·

δ) να προσδιορίζει συνθήκες και δείκτες που συσχετίζονται συχνά με κυβερνοεπιθέσεις στον τομέα της ηλεκτρικής ενέργειας·

ε) να καθορίζει αν πρέπει να διενεργηθεί περαιτέρω ανάλυση και να ληφθούν προληπτικά μέτρα μέσω της αξιολόγησης και του προσδιορισμού των παραγόντων κινδύνου·

στ) να ενημερώνει τις αρμόδιες αρχές σχετικά με τους κινδύνους που έχουν εντοπιστεί και τις συνιστώμενες προληπτικές ενέργειες που αφορούν ειδικά τις ενδιαφερόμενες οντότητες·

ζ) να ενημερώνει όλες τις σχετικές οντότητες που αναφέρονται στο άρθρο 2 όσον αφορά τα αποτελέσματα των πληροφοριών που αξιολογούνται σύμφωνα με τα στοιχεία β), γ) και δ) της παρούσας παραγράφου·

η) να περιλαμβάνει περιοδικά τις σχετικές πληροφορίες στην έκθεση επίγνωσης της κατάστασης, η οποία εκδίδεται σύμφωνα με το άρθρο 7 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881·

θ) να αντλεί, όπου είναι δυνατόν, συναφή δεδομένα που υποδεικνύουν δυνητική παραβίαση ασφάλειας ή κυβερνοεπίθεση (δείκτες παραβίασης) από τις συλλεγόμενες πληροφορίες.

3. Οι CSIRT διαδίδουν τις πληροφορίες που λαμβάνουν από τον ENISA στις ενδιαφερόμενες οντότητες χωρίς καθυστέρηση, στο πλαίσιο των οικείων καθηκόντων που ορίζονται στο άρθρο 11 παράγραφος 3 στοιχείο β) της οδηγίας (ΕΕ) 2022/2555.

4. Ο ACER παρακολουθεί την αποτελεσματικότητα των ECEAC. Ο ENISA συνδράμει τον ACER παρέχοντας όλες τις απαραίτητες πληροφορίες, σύμφωνα με το άρθρο 6 παράγραφος 2 και το άρθρο 7 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881. Η ανάλυση της εν λόγω δραστηριότητας παρακολούθησης αποτελεί μέρος της παρακολούθησης σύμφωνα με το άρθρο 12 του παρόντος κανονισμού.

ΚΕΦΑΛΑΙΟ VI

ΠΛΑΙΣΙΟ ΑΣΚΗΣΕΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

Άρθρο 43

Ασκήσεις κυβερνοασφάλειας σε επίπεδο οντότητας και κράτους μέλους

1. Έως τις 31 Δεκεμβρίου του έτους μετά την κοινοποίηση των οντοτήτων κρίσιμου αντικτύπου και, στη συνέχεια, ανά τριετία, κάθε οντότητα κρίσιμου αντικτύπου διενεργεί άσκηση κυβερνοασφάλειας, η οποία περιλαμβάνει ένα ή περισσότερα σενάρια με κυβερνοεπιθέσεις που επηρεάζουν άμεσα ή έμμεσα τις διασυνοριακές ροές ηλεκτρικής ενέργειας και σχετίζονται με τους κινδύνους που εντοπίζονται κατά τις εκτιμήσεις κινδύνων για την κυβερνοασφάλεια σε επίπεδο κράτους μέλους και οντότητας σύμφωνα με το άρθρο 20 και το άρθρο 27.

2. Κατά παρέκκλιση από την παράγραφο 1, η ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων, αφού ζητήσει τη γνώμη της αρμόδιας αρχής και της σχετικής αρχής διαχείρισης κυβερνοκρίσεων, όπως ορίζεται ή θεσπίζεται με την οδηγία (ΕΕ) 2022/2555, δυνάμει του άρθρου 9, μπορεί να αποφασίσει να οργανώσει άσκηση κυβερνοασφάλειας σε επίπεδο κράτους μέλους, όπως περιγράφεται στην παράγραφο 1, αντί να διενεργήσει την άσκηση κυβερνοασφάλειας σε επίπεδο οντότητας. Στο πλαίσιο αυτό, η αρμόδια αρχή ενημερώνει:

α) όλες τις οντότητες κρίσιμου αντικτύπου του οικείου κράτους μέλους, την εθνική ρυθμιστική αρχή, τις CSIRT και την ΕΑΑ κυβερνοασφάλειας, το αργότερο έως τις 30 Ιουνίου του έτους που προηγείται της άσκησης κυβερνοασφάλειας σε επίπεδο οντότητας·

β) κάθε οντότητα που συμμετέχει στην άσκηση κυβερνοασφάλειας σε επίπεδο κράτους μέλους, το αργότερο 6 μήνες πριν από τη διεξαγωγή της.

3. Η ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων, με την τεχνική υποστήριξη των οικείων CSIRT, οργανώνει την άσκηση κυβερνοασφάλειας που περιγράφεται στην παράγραφο 2 σε επίπεδο κράτους μέλους ανεξάρτητα ή στο πλαίσιο διαφορετικής άσκησης κυβερνοασφάλειας στο εν λόγω κράτος μέλος. Προκειμένου να είναι σε θέση να ομαδοποιήσει τις ασκήσεις αυτές, η ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων μπορεί να αναβάλει κατά ένα έτος την άσκηση κυβερνοασφάλειας σε επίπεδο κράτους μέλους που αναφέρεται στην παράγραφο 1.

4. Οι ασκήσεις κυβερνοασφάλειας σε επίπεδο οντότητας και σε επίπεδο κράτους μέλους συνάδουν με τα εθνικά πλαίσια διαχείρισης κρίσεων κυβερνοασφάλειας σύμφωνα με το άρθρο 9 παράγραφος 4 στοιχείο δ) της οδηγίας (ΕΕ) 2022/2555.

5. Έως τις 31ης Δεκεμβρίου 2026 και, στη συνέχεια, ανά τριετία, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καθιστά διαθέσιμο υπόδειγμα σεναρίου άσκησης για τη διεξαγωγή των ασκήσεων κυβερνοασφάλειας σε επίπεδο οντότητας και κράτους μέλους που αναφέρονται στην παράγραφο 1. Το υπόδειγμα αυτό λαμβάνει υπόψη τα αποτελέσματα της πιο πρόσφατης εκτίμησης κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας και κράτους μέλους και περιλαμβάνει καίρια κριτήρια επιτυχίας. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ διασφαλίζουν τη συμμετοχή του ACER και του ENISA στην κατάρτιση του εν λόγω υποδείγματος.

Άρθρο 44

Περιφερειακές ή διαπεριφερειακές ασκήσεις κυβερνοασφάλειας

1. Έως τις 31ης Δεκεμβρίου 2029 και, στη συνέχεια, ανά τριετία, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, διοργανώνει περιφερειακή άσκηση κυβερνοασφάλειας σε κάθε λειτουργική περιφέρεια του συστήματος. Οι οντότητες κρίσιμου αντικτύπου στη λειτουργική περιφέρεια του συστήματος συμμετέχουν στην περιφερειακή άσκηση κυβερνοασφάλειας. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, μπορεί να διοργανώνει, αντί περιφερειακής άσκησης κυβερνοασφάλειας, διαπεριφερειακή άσκηση κυβερνοασφάλειας σε περισσότερες από μία λειτουργικές περιφέρειες του συστήματος εντός του ίδιου χρονικού πλαισίου. Η άσκηση θα πρέπει να λαμβάνει υπόψη άλλες υφιστάμενες εκτιμήσεις και σενάρια κινδύνων για την κυβερνοασφάλεια που έχουν εκπονηθεί σε επίπεδο Ένωσης.

2. Ο ENISA υποστηρίζει το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ κατά την προετοιμασία και την οργάνωση της άσκησης κυβερνοασφάλειας σε περιφερειακό ή διαπεριφερειακό επίπεδο.

3. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συντονισμό με τον φορέα ΔΣΔ της ΕΕ, ενημερώνει τις οντότητες κρίσιμου αντικτύπου που συμμετέχουν στην περιφερειακή ή διαπεριφερειακή άσκηση κυβερνοασφάλειας έξι μήνες πριν από τη διενέργεια της άσκησης.

4. Ο διοργανωτής τακτικής άσκησης κυβερνοασφάλειας σε επίπεδο Ένωσης σύμφωνα με το άρθρο 7 παράγραφος 5 του κανονισμού (ΕΕ) 2019/881 ή οποιασδήποτε υποχρεωτικής άσκησης κυβερνοασφάλειας που σχετίζεται με τον τομέα της ηλεκτρικής ενέργειας εντός της ίδιας γεωγραφικής περιμέτρου μπορεί να καλέσει το ΕΔΔΣΜ ηλεκτρικής ενέργειας και τον φορέα ΔΣΔ της ΕΕ να συμμετάσχουν. Στις περιπτώσεις αυτές, δεν εφαρμόζεται η υποχρέωση της παραγράφου 1, υπό την προϋπόθεση ότι στην ίδια άσκηση συμμετέχουν όλες οι οντότητες κρίσιμου αντικτύπου στη λειτουργική περιφέρεια του συστήματος.

5. Εάν το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ συμμετέχουν σε άσκηση κυβερνοασφάλειας που αναφέρεται στην παράγραφο 4, μπορούν να αναβάλουν την περιφερειακή ή διαπεριφερειακή άσκηση κυβερνοασφάλειας που αναφέρεται στην παράγραφο 1 κατά ένα έτος.

6. Έως τις 31ης Δεκεμβρίου 2027 και, στη συνέχεια, ανά τριετία, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συντονισμό με τον φορέα ΔΣΔ της ΕΕ, καθιστά διαθέσιμο υπόδειγμα άσκησης για τη διεξαγωγή των περιφερειακών και διαπεριφερειακών ασκήσεων κυβερνοασφάλειας. Το υπόδειγμα αυτό λαμβάνει υπόψη τα αποτελέσματα της πιο πρόσφατης εκτίμησης κινδύνων για την κυβερνοασφάλεια σε περιφερειακό επίπεδο και περιλαμβάνει καίρια κριτήρια επιτυχίας. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας ζητεί τη γνώμη της Επιτροπής και μπορεί να ζητήσει συμβουλές από τον ACER, τον ENISA και το Κοινό Κέντρο Ερευνών σχετικά με την οργάνωση και την εκτέλεση των περιφερειακών και διαπεριφερειακών ασκήσεων κυβερνοασφάλειας.

Άρθρο 45

Αποτελέσματα ασκήσεων κυβερνοασφάλειας σε επίπεδο οντότητας, κράτους μέλους, σε περιφερειακό ή διαπεριφερειακό επίπεδο

1. Κατόπιν αιτήματος οντότητας κρίσιμου αντικτύπου, οι πάροχοι κρίσιμων υπηρεσιών συμμετέχουν στις ασκήσεις κυβερνοασφάλειας που αναφέρονται στο άρθρο 43 παράγραφοι 1 και 2 και στο άρθρο 44 παράγραφος 1, όταν παρέχουν υπηρεσίες για την οντότητα κρίσιμου αντικτύπου στον τομέα που αντιστοιχεί στο πεδίο εφαρμογής της σχετικής άσκησης κυβερνοασφάλειας.

2. Οι διοργανωτές των ασκήσεων κυβερνοασφάλειας που αναφέρονται στο άρθρο 43 παράγραφοι 1 και 2 και στο άρθρο 44 παράγραφος 1, με τις συμβουλές του ENISA, εφόσον τις ζητήσουν, και σύμφωνα με το άρθρο 7 παράγραφος 5 του κανονισμού (ΕΕ) 2019/881, αναλύουν και οριστικοποιούν τη σχετική άσκηση κυβερνοασφάλειας μέσω έκθεσης στην οποία συνοψίζονται τα διδάγματα και η οποία απευθύνεται σε όλους τους συμμετέχοντες. Η έκθεση περιλαμβάνει:

α) τα σενάρια της άσκησης, αναφορές συνεδριάσεων, τις κύριες θέσεις, επιτυχίες και διδάγματα που αντλήθηκαν σε οποιοδήποτε επίπεδο της αξιακής αλυσίδας της ηλεκτρικής ενέργειας·

β) διαπίστωση της εκπλήρωσης ή όχι των βασικών κριτηρίων επιτυχίας·

γ) κατάλογο συστάσεων προς τις οντότητες που συμμετείχαν στη σχετική άσκηση κυβερνοασφάλειας με σκοπό τη διόρθωση, την προσαρμογή ή την αλλαγή διεργασιών, διαδικασιών χειρισμού κρίσεων κυβερνοασφάλειας, συναφών μοντέλων διακυβέρνησης και τυχόν υφιστάμενων συμβατικών δεσμεύσεων με παρόχους κρίσιμων υπηρεσιών.

3. Εάν ζητηθεί από το δίκτυο CSIRT, την Ομάδα Συνεργασίας NIS ή το EU-CyCLONe, οι διοργανωτές των ασκήσεων κυβερνοασφάλειας που αναφέρονται στο άρθρο 43 παράγραφοι 1 και 2 και στο άρθρο 44 παράγραφος 1 κοινοποιούν το αποτέλεσμα της σχετικής άσκησης κυβερνοασφάλειας. Οι διοργανωτές κοινοποιούν σε κάθε οντότητα που συμμετείχε στις ασκήσεις τις πληροφορίες που αναφέρονται στην παράγραφο 2 στοιχεία α) και β) του παρόντος άρθρου. Οι διοργανωτές κοινοποιούν τον κατάλογο των συστάσεων που αναφέρονται στην εν λόγω παράγραφο στοιχείο γ) αποκλειστικά στις οντότητες στις οποίες απευθύνονται οι συστάσεις.

4. Οι διοργανωτές των ασκήσεων κυβερνοασφάλειας που αναφέρονται στο άρθρο 43 παράγραφοι 1 και 2 και στο άρθρο 44 παράγραφος 1 παρακολουθούν τακτικά, μαζί με τις οντότητες που συμμετείχαν στις ασκήσεις, την εφαρμογή των συστάσεων σύμφωνα με την παράγραφο 2 στοιχείο γ) του παρόντος άρθρου.

ΚΕΦΑΛΑΙΟ VII

ΠΡΟΣΤΑΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 46

Αρχές για την προστασία των ανταλλασσόμενων πληροφοριών

1. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 διασφαλίζουν ότι οι πληροφορίες που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού είναι προσβάσιμες μόνο βάσει της ανάγκης για γνώση και σύμφωνα με τους σχετικούς ενωσιακούς και εθνικούς κανόνες για την ασφάλεια των πληροφοριών.

2. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 διασφαλίζουν ότι διενεργείται χειρισμός και παρακολούθηση των πληροφοριών που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού καθ' όλη τη διάρκεια του κύκλου ζωής των εν λόγω πληροφοριών και ότι αυτές μπορούν να δημοσιοποιηθούν στο τέλος του κύκλου ζωής τους μόνο μετά την ανωνυμοποίησή τους.

3. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 διασφαλίζουν ότι εφαρμόζονται όλα τα αναγκαία μέτρα προστασίας οργανωτικού και τεχνικού χαρακτήρα για τη διασφάλιση και την προστασία της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της μη άρνησης αναγνώρισης των πληροφοριών που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού, ανεξάρτητα από τα μέσα που χρησιμοποιούνται. Τα μέτρα προστασίας:

α) είναι αναλογικά·

β) λαμβάνουν υπόψη τους κινδύνους για την κυβερνοασφάλεια που σχετίζονται με γνωστές παρελθούσες και αναδυόμενες απειλές στις οποίες ενδέχεται να υπόκεινται οι εν λόγω πληροφορίες στο πλαίσιο του παρόντος κανονισμού·

γ) στο μέτρο του δυνατού, βασίζονται σε εθνικά, ευρωπαϊκά ή διεθνή πρότυπα και βέλτιστες πρακτικές·

δ) είναι τεκμηριωμένα.

4. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 διασφαλίζουν ότι κάθε πρόσωπο στο οποίο χορηγείται πρόσβαση σε πληροφορίες που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού ενημερώνεται για τους κανόνες ασφάλειας που ισχύουν σε επίπεδο οντότητας και για τα μέτρα και τις διαδικασίες που σχετίζονται με την προστασία των πληροφοριών. Οι εν λόγω οντότητες διασφαλίζουν ότι το ενδιαφερόμενο πρόσωπο αναγνωρίζει την ευθύνη για την προστασία των πληροφοριών σύμφωνα με τις οδηγίες που δόθηκαν κατά τη διάρκεια της ενημέρωσης.

5. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 διασφαλίζουν ότι η πρόσβαση στις πληροφορίες που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού περιορίζεται σε πρόσωπα:

α) τα οποία είναι εξουσιοδοτημένα να έχουν πρόσβαση στις πληροφορίες αυτές βάσει των καθηκόντων τους και περιορίζονται στην εκτέλεση των καθηκόντων που τους έχουν ανατεθεί·

β) για τα οποία η οντότητα ήταν σε θέση να αξιολογήσει αρχές δεοντολογίας και ακεραιότητας, καθώς και για τα οποία δεν υπάρχουν αποδεικτικά στοιχεία αρνητικού αποτελέσματος από έλεγχο επαλήθευσης ιστορικού για την αξιολόγηση της αξιοπιστίας των ατόμων σύμφωνα με τις βέλτιστες πρακτικές και τις τυπικές απαιτήσεις ασφάλειας της οντότητας και, κατά περίπτωση, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

6. Οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 έχουν τη γραπτή συμφωνία του φυσικού ή νομικού προσώπου που αρχικά δημιούργησε ή παρείχε τις πληροφορίες, πριν από την παροχή των εν λόγω πληροφοριών σε τρίτο μέρος που δεν εμπίπτει στο πεδίο εφαρμογής του παρόντος κανονισμού.

7. Κάθε οντότητα που αναφέρεται στο άρθρο 2 παράγραφος 1 μπορεί να θεωρήσει ότι οι πληροφορίες αυτές κοινοποιούνται χωρίς συμμόρφωση με τις παραγράφους 1 και 4 του παρόντος άρθρου, προκειμένου να αποτραπεί ταυτόχρονη κρίση ηλεκτρικής ενέργειας της οποίας τα βαθύτερα αίτια εμπίπτουν στο πεδίο της κυβερνοασφάλειας ή οποιαδήποτε διασυνοριακή κρίση εντός της Ένωσης σε άλλον τομέα. Στην περίπτωση αυτή:

α) ζητεί τη γνώμη της αρμόδιας αρχής και εξουσιοδοτείται από αυτήν να κοινοποιήσει τις εν λόγω πληροφορίες·

β) ανωνυμοποιεί τις εν λόγω πληροφορίες χωρίς αυτές να απολέσουν τα στοιχεία που είναι απαραίτητα για την ενημέρωση του κοινού σχετικά με επικείμενο και σοβαρό κίνδυνο για τις διασυνοριακές ροές ηλεκτρικής ενέργειας και τα πιθανά μέτρα μετριασμού·

γ) διαφυλάσσει την ταυτότητα του φορέα προέλευσης και των οντοτήτων που επεξεργάζονται τις εν λόγω πληροφορίες δυνάμει του παρόντος κανονισμού.

8. Κατά παρέκκλιση από την παράγραφο 6 του παρόντος άρθρου, οι αρμόδιες αρχές μπορούν να παρέχουν πληροφορίες που παρέχονται, λαμβάνονται, ανταλλάσσονται ή διαβιβάζονται δυνάμει του παρόντος κανονισμού σε τρίτο μέρος που δεν περιλαμβάνεται στο άρθρο 2 παράγραφος 1 χωρίς τη γραπτή προηγούμενη συγκατάθεση του φορέα προέλευσης των πληροφοριών, αλλά τον ενημερώνουν το συντομότερο δυνατόν. Πριν από τη γνωστοποίηση πληροφοριών που έχουν παρασχεθεί, ληφθεί, ανταλλαγεί ή διαβιβαστεί δυνάμει του παρόντος κανονισμού σε τρίτο μέρος που δεν αναφέρεται στο άρθρο 2 παράγραφος 1, η ενδιαφερόμενη αρμόδια αρχή διασφαλίζει εύλογα ότι το ενδιαφερόμενο τρίτο μέρος γνωρίζει τους ισχύοντες κανόνες ασφάλειας και λαμβάνει εύλογη διαβεβαίωση ότι το ενδιαφερόμενο τρίτο μέρος μπορεί να προστατεύσει τις ληφθείσες πληροφορίες σύμφωνα με τις παραγράφους 1 έως 5 του παρόντος άρθρου. Η αρμόδια αρχή ανωνυμοποιεί τις εν λόγω πληροφορίες χωρίς αυτές να απολέσουν τα στοιχεία που είναι αναγκαία για την ενημέρωση του κοινού σχετικά με επικείμενο και σοβαρό κίνδυνο για τις διασυνοριακές ροές ηλεκτρικής ενέργειας και τα πιθανά μέτρα μετριασμού, και διαφυλάσσει την ταυτότητα του φορέα προέλευσης των πληροφοριών. Στην περίπτωση αυτήν, το τρίτο μέρος που δεν αναφέρεται στο άρθρο 2 παράγραφος 1 προστατεύει τις ληφθείσες πληροφορίες σύμφωνα με τις διατάξεις που ισχύουν ήδη σε επίπεδο οντότητας ή, όταν αυτό δεν είναι δυνατόν, σύμφωνα με τις διατάξεις και τις οδηγίες που παρέχονται από τη σχετική αρμόδια αρχή.

9. Το παρόν άρθρο δεν εφαρμόζεται σε οντότητες που δεν αναφέρονται στο άρθρο 2 παράγραφος 1 οι οποίες λαμβάνουν πληροφορίες σύμφωνα με την παράγραφο 6 του παρόντος άρθρου. Στην περίπτωση αυτήν, εφαρμόζεται η παράγραφος 7 του παρόντος άρθρου ή η αρμόδια αρχή μπορεί να παράσχει στην εν λόγω οντότητα γραπτές διατάξεις που θα εφαρμόζονται σε περιπτώσεις λήψης πληροφοριών σύμφωνα με τον παρόντα κανονισμό.

Άρθρο 47

Εμπιστευτικότητα των πληροφοριών

1. Κάθε πληροφορία που παρέχεται, λαμβάνεται, ανταλλάσσεται ή διαβιβάζεται σύμφωνα με τον παρόντα κανονισμό υπόκειται στους όρους επαγγελματικού απορρήτου που καθορίζονται στις παραγράφους 2 έως 5 του παρόντος άρθρου του παρόντος κανονισμού και στις απαιτήσεις του άρθρου 65 του κανονισμού (ΕΕ) 2019/943. Κάθε πληροφορία που παρέχεται, λαμβάνεται, ανταλλάσσεται ή διαβιβάζεται μεταξύ των οντοτήτων που αναφέρονται στο άρθρο 2 του παρόντος κανονισμού, για τους σκοπούς της εφαρμογής του παρόντος κανονισμού, προστατεύεται, λαμβανομένου υπόψη του επιπέδου εμπιστευτικότητας των πληροφοριών που εφαρμόζει ο φορέας προέλευσης.

2. Η υποχρέωση τήρησης του επαγγελματικού απορρήτου ισχύει για τις οντότητες που αναφέρονται στο άρθρο 2.

3. Οι ΕΑΑ κυβερνοασφάλειας, οι εθνικές ρυθμιστικές αρχές, οι ΕΑΑ ετοιμότητας αντιμετώπισης κινδύνων και οι CSIRT ανταλλάσσουν όλες τις απαραίτητες πληροφορίες για την εκτέλεση των καθηκόντων τους.

4. Κάθε πληροφορία που λαμβάνεται, ανταλλάσσεται ή διαβιβάζεται μεταξύ των οντοτήτων που αναφέρονται στο άρθρο 2 παράγραφος 1, για τους σκοπούς της εφαρμογής του άρθρου 23, είναι ανωνυμοποιημένη και συγκεντρωτική.

5. Οι πληροφορίες που λαμβάνει οποιαδήποτε οντότητα ή αρχή που υπόκειται στον παρόντα κανονισμό κατά την εκτέλεση των καθηκόντων της δεν γνωστοποιούνται σε καμία άλλη οντότητα ή αρχή, με την επιφύλαξη των περιπτώσεων που καλύπτονται από το εθνικό δίκαιο, άλλες διατάξεις του παρόντος κανονισμού ή άλλη σχετική νομοθεσία της Ένωσης.

6. Με την επιφύλαξη της εθνικής ή της ενωσιακής νομοθεσίας, μια αρχή, μια οντότητα ή ένα φυσικό πρόσωπο που λαμβάνει πληροφορίες σύμφωνα με τον παρόντα κανονισμό δεν επιτρέπεται να τις χρησιμοποιεί για κανέναν άλλο σκοπό εκτός από την εκτέλεση των καθηκόντων του δυνάμει του παρόντος κανονισμού.

7. Ο ACER, αφού ζητήσει τη γνώμη του ENISA, όλων των αρμόδιων αρχών, του ΕΔΔΣΜ ηλεκτρικής ενέργειας και του φορέα ΔΣΔ της ΕΕ, εκδίδει έως τις 13 Ιουνίου 2025 κατευθυντήριες γραμμές σχετικά με τους μηχανισμούς ανταλλαγής πληροφοριών από όλες τις οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1, και ιδίως τις προβλεπόμενες ροές επικοινωνίας, καθώς και μεθόδους για την ανωνυμοποίηση και τη συγκέντρωση πληροφοριών για τους σκοπούς της εφαρμογής του παρόντος άρθρου.

8. Πληροφορίες που είναι εμπιστευτικές σύμφωνα με τους ενωσιακούς και τους εθνικούς κανόνες ανταλλάσσονται με την Επιτροπή και με άλλες αρμόδιες αρχές μόνο εφόσον η εν λόγω ανταλλαγή είναι αναγκαία για την εφαρμογή του παρόντος κανονισμού. Οι ανταλλασσόμενες πληροφορίες περιορίζονται σε ό,τι είναι αναγκαίο και αναλογικό προς τον σκοπό της εν λόγω ανταλλαγής. Η ανταλλαγή πληροφοριών διαφυλάσσει την εμπιστευτικότητα αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των οντοτήτων κρίσιμου ή υψηλού αντικτύπου.

ΚΕΦΑΛΑΙΟ VIII

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 48

Προσωρινές διατάξεις

1. Έως την έγκριση των όρων και προϋποθέσεων ή των μεθοδολογιών που αναφέρονται στο άρθρο 6 παράγραφος 2 ή των σχεδίων που αναφέρονται στο άρθρο 6 παράγραφος 3, το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζει μη δεσμευτική καθοδήγηση σχετικά με τα ακόλουθα ζητήματα:

α) προσωρινό δείκτη αντικτύπου στην κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας (στο εξής: ECII) σύμφωνα με την παράγραφο 2 του παρόντος άρθρου·

β) προσωρινό κατάλογο διαδικασιών υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης σύμφωνα με την παράγραφο 4 του παρόντος άρθρου· και

γ) προσωρινό κατάλογο ευρωπαϊκών και διεθνών προτύπων και ελέγχων που απαιτούνται από την εθνική νομοθεσία και αφορούν πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας σύμφωνα με την παράγραφο 6 του παρόντος άρθρου.

2. Έως τις 13ης Οκτωβρίου 2024 το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζει σύσταση για προσωρινό ECII. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, κοινοποιεί τον συνιστώμενο προσωρινό ECII στις αρμόδιες αρχές.

3. Τέσσερις μήνες από την παραλαβή του συνιστώμενου προσωρινού ECII ή το αργότερο έως τις 13ης Φεβρουαρίου 2025, οι αρμόδιες αρχές προσδιορίζουν οντότητες υποψήφιες να χαρακτηριστούν ως υψηλού ή κρίσιμου αντικτύπου στο οικείο κράτος μέλος με βάση τον συνιστώμενο ECII και καταρτίζουν προσωρινό κατάλογο οντοτήτων υψηλού ή κρίσιμου αντικτύπου. Οι οντότητες υψηλού ή κρίσιμου αντικτύπου που περιλαμβάνονται στον προσωρινό κατάλογο μπορούν να εκπληρώνουν οικειοθελώς τις υποχρεώσεις τους όπως ορίζονται στον παρόντα κανονισμό βάσει της αρχής της προφύλαξης. Έως τις 13ης Μαρτίου 2025 οι αρμόδιες αρχές κοινοποιούν στις οντότητες που περιλαμβάνονται στον προσωρινό κατάλογο ότι έχουν χαρακτηριστεί ως οντότητες υψηλού ή κρίσιμου αντικτύπου.

4. Έως τις 13ης Δεκεμβρίου 2024 το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζει προσωρινό κατάλογο διαδικασιών υψηλού ή κρίσιμου αντικτύπου σε επίπεδο Ένωσης. Οι οντότητες που λαμβάνουν κοινοποίηση σύμφωνα με την παράγραφο 3 οι οποίες αποφασίζουν οικειοθελώς να εκπληρώσουν τις υποχρεώσεις τους, όπως ορίζονται στον παρόντα κανονισμό βάσει της αρχής της προφύλαξης, χρησιμοποιούν τον προσωρινό κατάλογο διαδικασιών υψηλού ή κρίσιμου αντικτύπου για τον καθορισμό των προσωρινών περιμέτρων υψηλού ή κρίσιμου αντικτύπου και για τον προσδιορισμό των περιουσιακών στοιχείων που πρέπει να συμπεριληφθούν στην πρώτη εκτίμηση των κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας.

5. Έως τις 13 Σεπτεμβρίου 2024 κάθε αρμόδια αρχή σύμφωνα με το άρθρο 4 παράγραφος 1 παρέχει στο ΕΔΔΣΜ ηλεκτρικής ενέργειας και στον φορέα ΔΣΔ της ΕΕ κατάλογο της εθνικής της νομοθεσίας που αφορά πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας.

6. Έως τις 13 Ιουνίου 2025 το ΕΔΔΣΜ ηλεκτρικής ενέργειας, σε συνεργασία με τον φορέα ΔΣΔ της ΕΕ, καταρτίζει προσωρινό κατάλογο ευρωπαϊκών και διεθνών προτύπων και ελέγχων που απαιτούνται από την εθνική νομοθεσία και αφορούν πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας, λαμβάνοντας υπόψη τις πληροφορίες που παρέχουν οι αρμόδιες αρχές.

7. Ο προσωρινός κατάλογος ευρωπαϊκών και διεθνών προτύπων και ελέγχων περιλαμβάνει:

α) ευρωπαϊκά και διεθνή πρότυπα και εθνική νομοθεσία που παρέχουν καθοδήγηση σχετικά με τις μεθοδολογίες διαχείρισης των κινδύνων για την κυβερνοασφάλεια σε επίπεδο οντότητας· και

β) ελέγχους στο πεδίο της κυβερνοασφάλειας, ισοδύναμους με τους ελέγχους που αναμένεται να αποτελέσουν μέρος των ελάχιστων και των προηγμένων ελέγχων κυβερνοασφάλειας.

8. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ λαμβάνουν υπόψη τις απόψεις του ENISA και του ACER κατά την οριστικοποίηση του προσωρινού καταλόγου προτύπων. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ δημοσιεύουν τον μεταβατικό κατάλογο ευρωπαϊκών και διεθνών προτύπων και ελέγχων στους οικείους δικτυακούς τόπους.

9. Το ΕΔΔΣΜ ηλεκτρικής ενέργειας και ο φορέας ΔΣΔ της ΕΕ ζητούν τη γνώμη του ENISA και του ACER σχετικά με τις προτάσεις για μη δεσμευτική καθοδήγηση που καταρτίζεται σύμφωνα με την παράγραφο 1.

10. Έως ότου αναπτυχθούν οι ελάχιστοι και οι προηγμένοι έλεγχοι κυβερνοασφάλειας σύμφωνα με το άρθρο 29 και εγκριθούν σύμφωνα με το άρθρο 8, όλες οι οντότητες που αναφέρονται στο άρθρο 2 παράγραφος 1 προσπαθούν να εφαρμόσουν σταδιακά τη μη δεσμευτική καθοδήγηση που καταρτίζεται σύμφωνα με την παράγραφο 1.

Άρθρο 49

Έναρξη ισχύος

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

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

Βρυξέλλες, 11 Μαρτίου 2024.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN