Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/2690

18.10.2024

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/2690 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 17ης Οκτωβρίου 2024

για τη θέσπιση κανόνων εφαρμογής της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη την 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) ([1]), και ιδίως το άρθρο 21 παράγραφος 5 πρώτο εδάφιο και το άρθρο 23 παράγραφος 11 δεύτερο εδάφιο,

Εκτιμώντας τα ακόλουθα:

(1) Όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης, όπως καλύπτονται από το άρθρο 3 της οδηγίας (ΕΕ) 2022/2555 (στο εξής: σχετικές οντότητες), ο παρών κανονισμός αποσκοπεί στον καθορισμό των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων που αναφέρονται στο άρθρο 21 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555 και στον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θα πρέπει να θεωρείται σημαντικό, όπως αναφέρεται στο άρθρο 23 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555.

(2) Λαμβάνοντας υπόψη τον διασυνοριακό χαρακτήρα των δραστηριοτήτων τους και προκειμένου να διασφαλιστεί ένα συνεκτικό πλαίσιο για τους παρόχους υπηρεσιών εμπιστοσύνης, ο παρών κανονισμός θα πρέπει, όσον αφορά τους παρόχους υπηρεσιών εμπιστοσύνης, να προσδιορίσει περαιτέρω τις περιπτώσεις στις οποίες ένα περιστατικό θεωρείται σημαντικό, πέραν του καθορισμού των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.

(3) Σύμφωνα με το άρθρο 21 παράγραφος 5 τρίτο εδάφιο της οδηγίας (ΕΕ) 2022/2555, οι τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού βασίζονται σε ευρωπαϊκά και διεθνή πρότυπα, όπως τα πρότυπα ISO/IEC 27001, ISO/IEC 27002 και ETSI EN 319401, και σε τεχνικές προδιαγραφές, όπως οι προδιαγραφές CEN/TS 18026:2024, σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

(4) Όσον αφορά την υλοποίηση και την εφαρμογή των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού, σύμφωνα με την αρχή της αναλογικότητας, θα πρέπει να λαμβάνεται δεόντως υπόψη ο διαφορετικός βαθμός έκθεσης στον κίνδυνο των σχετικών οντοτήτων, όπως η κρισιμότητα της σχετικής οντότητας, οι κίνδυνοι στους οποίους είναι εκτεθειμένη, το μέγεθος και η δομή της σχετικής οντότητας, καθώς και η πιθανότητα εμφάνισης περιστατικών και η σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους, κατά τη συμμόρφωση με τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού.

([1]) ΕΕ L 333 της 27.12.2022, σ. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) Σύμφωνα με την αρχή της αναλογικότητας, όταν οι σχετικές οντότητες δεν μπορούν να εφαρμόσουν ορισμένες από τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας λόγω του μεγέθους τους, οι εν λόγω οντότητες θα πρέπει να είναι σε θέση να λαμβάνουν άλλα αντισταθμιστικά μέτρα που είναι κατάλληλα για την επίτευξη του σκοπού των εν λόγω απαιτήσεων. Για παράδειγμα, κατά τον καθορισμό ρόλων, αρμοδιοτήτων και αρχών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών εντός της σχετικής οντότητας, οι πολύ μικρές οντότητες ενδέχεται να δυσκολεύονται να διαχωρίζουν τα συγκρουόμενα καθήκοντα και τους συγκρουόμενους τομείς ευθύνης. Οι εν λόγω οντότητες θα πρέπει να είναι σε θέση να εξετάζουν αντισταθμιστικά μέτρα, όπως στοχευμένη εποπτεία από τη διοίκηση της οντότητας ή αυξημένη παρακολούθηση και καταγραφή δεδομένων.

(6) Ορισμένες τεχνικές και μεθοδολογικές απαιτήσεις που ορίζονται στο παράρτημα του παρόντος κανονισμού θα πρέπει να εφαρμόζονται από τις σχετικές οντότητες κατά περίπτωση, όπου αρμόζει ή στον βαθμό που αυτό είναι εφικτό. Όταν μια σχετική οντότητα θεωρεί ότι δεν είναι κατάλληλο, δεν είναι σκόπιμο ή δεν είναι εφικτό για τη σχετική οντότητα να εφαρμόσει ορισμένες τεχνικές και μεθοδολογικές απαιτήσεις, όπως προβλέπεται στο παράρτημα του παρόντος κανονισμού, η σχετική οντότητα θα πρέπει να τεκμηριώνει με κατανοητό τρόπο το σκεπτικό της για τον σκοπό αυτό. Οι εθνικές αρμόδιες αρχές μπορούν, κατά την άσκηση της εποπτείας, να λαμβάνουν υπόψη τον κατάλληλο χρόνο που απαιτείται για την εφαρμογή από τις σχετικές οντότητες των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.

(7) Ο ENISA ή οι εθνικές αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2555 μπορούν να παρέχουν καθοδήγηση για την υποστήριξη των σχετικών οντοτήτων στον προσδιορισμό, στην ανάλυση και στην αξιολόγηση των κινδύνων με σκοπό την εφαρμογή των τεχνικών και μεθοδολογικών απαιτήσεων σχετικά με τη θέσπιση και τη διατήρηση κατάλληλου πλαισίου διαχείρισης κινδύνων. Η εν λόγω καθοδήγηση μπορεί να περιλαμβάνει, ιδίως, εθνικές και τομεακές εκτιμήσεις κινδύνου, καθώς και εκτιμήσεις κινδύνου ειδικά για ένα συγκεκριμένο είδος οντότητας. Η καθοδήγηση μπορεί επίσης να περιλαμβάνει εργαλεία ή υποδείγματα για την ανάπτυξη πλαισίου διαχείρισης κινδύνων στο επίπεδο των σχετικών οντοτήτων. Τα πλαίσια, η καθοδήγηση ή άλλοι μηχανισμοί που προβλέπονται από το εθνικό δίκαιο των κρατών μελών, καθώς και τα σχετικά ευρωπαϊκά και διεθνή πρότυπα, μπορούν επίσης να στηρίξουν τις σχετικές οντότητες στην απόδειξη της συμμόρφωσης με τον παρόντα κανονισμό. Επιπλέον, ο ENISA ή οι εθνικές αρμόδιες αρχές δυνάμει της οδηγίας (ΕΕ) 2022/2555 μπορούν να στηρίξουν τις σχετικές οντότητες στον προσδιορισμό και την εφαρμογή κατάλληλων λύσεων για την αντιμετώπιση των κινδύνων που προσδιορίζονται στις εν λόγω εκτιμήσεις κινδύνου. Η εν λόγω καθοδήγηση δεν θα πρέπει να θίγει την υποχρέωση των σχετικών οντοτήτων να προσδιορίζουν και να τεκμηριώνουν τους κινδύνους για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ούτε την υποχρέωση των σχετικών οντοτήτων να εφαρμόζουν τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού σύμφωνα με τις ανάγκες και τους πόρους τους.

(8) Τα μέτρα ασφάλειας δικτύου αφορούν: i) τη μετάβαση σε πρωτόκολλα επικοινωνίας επιπέδου δικτύου τελευταίας γενιάς, ii) την ανάπτυξη διεθνώς συμφωνημένων και διαλειτουργικών σύγχρονων προτύπων επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου και iii) την εφαρμογή βέλτιστων πρακτικών για την ασφάλεια του DNS και την ασφάλεια της δρομολόγησης στο διαδίκτυο και την υγιεινή της δρομολόγησης, συνεπάγονται δε ειδικές προκλήσεις όσον αφορά τον προσδιορισμό των βέλτιστων διαθέσιμων προτύπων και τεχνικών ανάπτυξης. Για να επιτευχθεί το συντομότερο δυνατόν υψηλό κοινό επίπεδο κυβερνοασφάλειας σε όλα τα δίκτυα, η Επιτροπή, με τη συνδρομή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και σε συνεργασία με τις αρμόδιες αρχές, τη βιομηχανία —συμπεριλαμβανομένου του κλάδου των τηλεπικοινωνιών— και άλλα ενδιαφερόμενα μέρη, θα πρέπει να στηρίξει την ανάπτυξη ενός πολυσυμμετοχικού φόρουμ με αποστολή τον προσδιορισμό αυτών των βέλτιστων διαθέσιμων προτύπων και τεχνικών ανάπτυξης. Η εν λόγω πολυσυμμετοχική καθοδήγηση δεν θα πρέπει να θίγει την υποχρέωση των σχετικών οντοτήτων να εφαρμόζουν τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού.

(9) Σύμφωνα με το άρθρο 21 παράγραφος 2 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555, οι βασικές και σημαντικές οντότητες θα πρέπει να διαθέτουν, εκτός από τις πολιτικές για την ανάλυση κινδύνου, πολιτικές για την ασφάλεια των συστημάτων πληροφοριών. Για τον σκοπό αυτό, οι σχετικές οντότητες θα πρέπει να θεσπίσουν πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, καθώς και πολιτικές για συγκεκριμένα θέματα, όπως πολιτικές ελέγχου πρόσβασης, οι οποίες θα πρέπει να συνάδουν με την πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Η πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών θα πρέπει να είναι έγγραφο ανώτατου επιπέδου που θα καθορίζει τη συνολική προσέγγιση των σχετικών οντοτήτων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών και θα πρέπει να εγκρίνεται από τα διοικητικά όργανα των σχετικών οντοτήτων. Οι πολιτικές για συγκεκριμένα θέματα θα πρέπει να εγκρίνονται από το κατάλληλο επίπεδο διοίκησης. Η πολιτική θα πρέπει να καθορίζει δείκτες και μέτρα για την παρακολούθηση της εφαρμογής της και της τρέχουσας κατάστασης του επιπέδου ωριμότητας της ασφάλειας δικτύου και πληροφοριών των σχετικών οντοτήτων, ιδίως για τη διευκόλυνση της εποπτείας της εφαρμογής των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας μέσω των διοικητικών οργάνων.

(10) Για τους σκοπούς των τεχνικών και μεθοδολογικών απαιτήσεων που ορίζονται στο παράρτημα του παρόντος κανονισμού, ο όρος «χρήστης» θα πρέπει να περιλαμβάνει όλα τα νομικά και φυσικά πρόσωπα που έχουν πρόσβαση στα συστήματα δικτύου και πληροφοριών της οντότητας.

(11) Για τον προσδιορισμό και την αντιμετώπιση των κινδύνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, οι σχετικές οντότητες θα πρέπει να θεσπίζουν και να διατηρούν κατάλληλο πλαίσιο διαχείρισης κινδύνων. Ως μέρος του πλαισίου διαχείρισης κινδύνων, οι σχετικές οντότητες θα πρέπει να καταρτίζουν, να εφαρμόζουν και να παρακολουθούν σχέδιο αντιμετώπισης κινδύνων. Οι σχετικές οντότητες μπορούν να χρησιμοποιούν το σχέδιο αντιμετώπισης κινδύνων για τον προσδιορισμό και την ιεράρχηση των επιλογών και των μέτρων όσον αφορά την αντιμετώπιση κινδύνων. Οι επιλογές για την αντιμετώπιση κινδύνων περιλαμβάνουν, ιδίως, την αποφυγή, τη μείωση ή, σε εξαιρετικές περιπτώσεις, την αποδοχή του κινδύνου. Η πρόκριση των επιλογών για την αντιμετώπιση κινδύνων θα πρέπει να λαμβάνει υπόψη τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται από τη σχετική οντότητα και να είναι σύμφωνη με την πολιτική της σχετικής οντότητας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Για την εφαρμογή των προκριθεισών επιλογών για την αντιμετώπιση κινδύνων, οι σχετικές οντότητες θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα αντιμετώπισης κινδύνων.

(12) Για τον εντοπισμό συμβάντων, παρ' ολίγον περιστατικών και περιστατικών, οι σχετικές οντότητες θα πρέπει να παρακολουθούν τα οικεία συστήματα δικτύου και πληροφοριών και να λαμβάνουν μέτρα για την αξιολόγηση συμβάντων, παρ' ολίγον περιστατικών και περιστατικών. Τα μέτρα αυτά θα πρέπει να είναι σε θέση να επιτρέπουν τον έγκαιρο εντοπισμό βασιζόμενων στο δίκτυο επιθέσεων με βάση πρότυπα ασύμμετρης εισερχόμενης και εξερχόμενης κίνησης και επιθέσεων άρνησης παροχής υπηρεσίας.

(13) Όταν οι σχετικές οντότητες διενεργούν ανάλυση επιχειρηματικών επιπτώσεων, ενθαρρύνονται να διενεργούν ολοκληρωμένη ανάλυση στην οποία καθορίζονται, κατά περίπτωση, ο μέγιστος ανεκτός χρόνος διακοπής, οι στόχοι ως προς τον χρόνο αποκατάστασης, οι στόχοι ως προς το σημείο αποκατάστασης και οι στόχοι για την παροχή υπηρεσιών.

(14) Προκειμένου να αμβλυνθούν οι κίνδυνοι που απορρέουν από την αλυσίδα εφοδιασμού μιας σχετικής οντότητας και τη σχέση της με τους προμηθευτές της, οι σχετικές οντότητες θα πρέπει να θεσπίσουν πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού η οποία θα διέπει τις σχέσεις τους με τους οικείους άμεσους προμηθευτές και παρόχους υπηρεσιών. Οι εν λόγω οντότητες θα πρέπει να προσδιορίζουν στις συμβάσεις με τους άμεσους προμηθευτές ή παρόχους υπηρεσιών επαρκείς ρήτρες ασφάλειας, για παράδειγμα απαιτώντας, κατά περίπτωση, μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 21 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555 ή άλλες παρόμοιες νομικές απαιτήσεις.

(15) Οι σχετικές οντότητες θα πρέπει να διενεργούν τακτικά δοκιμές ασφάλειας βάσει ειδικής πολιτικής και διαδικασιών για να επαληθεύουν κατά πόσον τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας εφαρμόζονται και λειτουργούν σωστά. Οι δοκιμές ασφάλειας μπορούν να διενεργούνται σε συγκεκριμένα συστήματα δικτύου και πληροφοριών ή στη σχετική οντότητα στο σύνολό της και μπορούν να περιλαμβάνουν αυτόματες ή χειροκίνητες δοκιμές, δοκιμές διείσδυσης, σάρωση ευπαθειών, στατικές και δυναμικές δοκιμές ασφάλειας εφαρμογών, δοκιμές παραμετροποίησης ή ελέγχους ασφαλείας. Οι σχετικές οντότητες μπορούν να διενεργούν δοκιμές ασφάλειας στα οικεία συστήματα δικτύου και πληροφοριών κατά την εγκατάσταση, μετά από αναβαθμίσεις ή τροποποιήσεις της υποδομής ή των εφαρμογών που θεωρούν σημαντικές, ή μετά από συντήρηση. Τα ευρήματα των δοκιμών ασφάλειας θα πρέπει να τεκμηριώνουν τις πολιτικές και τις διαδικασίες των σχετικών οντοτήτων για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, καθώς και ανεξάρτητες αξιολογήσεις των οικείων πολιτικών για την ασφάλεια δικτύου και πληροφοριών.

(16) Προκειμένου να αποφευχθούν σημαντικές διαταράξεις και βλάβες που προκαλούνται από την εκμετάλλευση μη αντιμετωπισθεισών ευπαθειών στα συστήματα δικτύου και πληροφοριών, οι σχετικές οντότητες θα πρέπει να καθορίζουν και να εφαρμόζουν κατάλληλες διαδικασίες διαχείρισης διορθώσεων ασφαλείας, οι οποίες ευθυγραμμίζονται με τις διαδικασίες διαχείρισης αλλαγών, διαχείρισης ευπαθειών και διαχείρισης κινδύνων και άλλες σχετικές διαδικασίες των σχετικών οντοτήτων. Οι σχετικές οντότητες θα πρέπει να λαμβάνουν μέτρα ανάλογα με τους οικείους πόρους για να διασφαλίζουν ότι οι διορθώσεις ασφαλείας δεν εισάγουν πρόσθετες ευπάθειες ή αστάθεια. Σε περίπτωση προγραμματισμένης αδυναμίας πρόσβασης στην υπηρεσία λόγω της εφαρμογής διορθώσεων ασφαλείας, οι σχετικές οντότητες ενθαρρύνονται να ενημερώνουν δεόντως τους πελάτες εκ των προτέρων.

(17) Οι σχετικές οντότητες θα πρέπει να διαχειρίζονται τους κινδύνους που απορρέουν από την απόκτηση προϊόντων ΤΠΕ ή υπηρεσιών ΤΠΕ από προμηθευτές ή παρόχους υπηρεσιών και θα πρέπει να εξασφαλίζουν ότι τα προϊόντα ΤΠΕ ή οι υπηρεσίες ΤΠΕ που πρόκειται να αποκτηθούν επιτυγχάνουν ορισμένα επίπεδα προστασίας της κυβερνοασφάλειας, για παράδειγμα με ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και δηλώσεις συμμόρφωσης ΕΕ για προϊόντα ΤΠΕ ή υπηρεσίες ΤΠΕ που εκδίδονται στο πλαίσιο ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας που εγκρίνεται δυνάμει του άρθρου 49 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]). Όταν οι σχετικές οντότητες καθορίζουν απαιτήσεις ασφάλειας που πρέπει να εφαρμόζονται στα προϊόντα ΤΠΕ που πρόκειται να αποκτηθούν, θα πρέπει να λαμβάνουν υπόψη τις ουσιώδεις απαιτήσεις κυβερνοασφάλειας που ορίζονται σε κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία.

(18) Για την προστασία από κυβερνοαπειλές και τη στήριξη της πρόληψης και του περιορισμού των παραβιάσεων δεδομένων, οι σχετικές οντότητες θα πρέπει να εφαρμόζουν λύσεις ασφάλειας δικτύου. Οι συνήθεις λύσεις για την ασφάλεια δικτύου περιλαμβάνουν τη χρήση τειχών προστασίας για την προστασία των εσωτερικών δικτύων των σχετικών οντοτήτων, τον περιορισμό των συνδέσεων και της πρόσβασης σε υπηρεσίες όπου οι συνδέσεις και η πρόσβαση είναι απολύτως αναγκαίες, καθώς και τη χρήση εικονικών ιδιωτικών δικτύων για εξ αποστάσεως πρόσβαση και τη δυνατότητα σύνδεσης των παρόχων υπηρεσιών μόνο μετά από αίτηση εξουσιοδότησης και για καθορισμένο χρονικό διάστημα, όπως η διάρκεια των εργασιών συντήρησης.

(19) Για την προστασία των δικτύων των σχετικών οντοτήτων και των οικείων συστημάτων πληροφοριών από κακόβουλο και μη εξουσιοδοτημένο λογισμικό, οι εν λόγω οντότητες θα πρέπει να εφαρμόζουν ελέγχους που αποτρέπουν ή εντοπίζουν τη χρήση μη εξουσιοδοτημένου λογισμικού και θα πρέπει, κατά περίπτωση, να χρησιμοποιούν λογισμικό εντοπισμού και απόκρισης. Οι σχετικές οντότητες θα πρέπει επίσης να εξετάσουν το ενδεχόμενο εφαρμογής μέτρων για την ελαχιστοποίηση της επιφάνειας επίθεσης, τη μείωση των ευπαθειών που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι, τον έλεγχο της εκτέλεσης εφαρμογών σε τελικά σημεία και την εγκατάσταση φίλτρων ηλεκτρονικού ταχυδρομείου και διαδικτυακών εφαρμογών για τη μείωση της έκθεσης σε κακόβουλο περιεχόμενο.

(20) Σύμφωνα με το άρθρο 21 παράγραφος 2 στοιχείο ζ) της οδηγίας (ΕΕ) 2022/2555, τα κράτη μέλη διασφαλίζουν ότι οι βασικές και σημαντικές οντότητες εφαρμόζουν βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια. Οι βασικές πρακτικές κυβερνοϋγιεινής μπορούν να περιλαμβάνουν τις αρχές μηδενικής εμπιστοσύνης, αναβαθμίσεις λογισμικού, την παραμετροποίηση συσκευών, την κατάτμηση δικτύου, τη διαχείριση ταυτοτήτων και πρόσβασης ή την ευαισθητοποίηση των χρηστών, την οργάνωση προγραμμάτων κατάρτισης για το προσωπικό τους και την ευαισθητοποίηση σχετικά με τις κυβερνοαπειλές, το ηλεκτρονικό ψάρεμα ή τις τεχνικές κοινωνικής μηχανικής. Οι πρακτικές κυβερνοϋγιεινής αποτελούν μέρος των διαφορετικών τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού. Όσον αφορά τις βασικές πρακτικές κυβερνοϋγιεινής για τους χρήστες, οι σχετικές οντότητες θα πρέπει να εξετάζουν πρακτικές όπως η πολιτική καθαρού γραφείου και καθαρής οθόνης, η χρήση πολυπαραγοντικής επαλήθευσης ταυτότητας και άλλων μέσων επαλήθευσης ταυτότητας, η ασφαλής χρήση ηλεκτρονικού ταχυδρομείου και η ασφαλής περιήγηση στο διαδίκτυο, η προστασία από το ηλεκτρονικό ψάρεμα και την κοινωνική μηχανική, οι πρακτικές ασφαλούς εξ αποστάσεως εργασίας.

(21) Προκειμένου να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση στα πάγια στοιχεία των σχετικών οντοτήτων, οι σχετικές οντότητες θα πρέπει να θεσπίσουν και να εφαρμόσουν ειδική επί του συγκεκριμένου θέματος πολιτική για την πρόσβαση προσώπων και συστημάτων δικτύου και πληροφοριών, όπως εφαρμογές.

(22) Προκειμένου να αποφευχθεί το ενδεχόμενο οι υπάλληλοι να μπορούν να κάνουν κατάχρηση, για παράδειγμα, των δικαιωμάτων πρόσβασης εντός της σχετικής οντότητας για να βλάψουν και να προκαλέσουν ζημία, οι σχετικές οντότητες θα πρέπει να εξετάσουν το ενδεχόμενο λήψης κατάλληλων μέτρων διαχείρισης της ασφάλειας των υπαλλήλων και να αυξήσουν την ευαισθητοποίηση του προσωπικού σχετικά με τους εν λόγω κινδύνους. Οι σχετικές οντότητες θα πρέπει να θεσπίζουν, να κοινοποιούν και να διατηρούν πειθαρχική διαδικασία για τη διαχείριση παραβιάσεων των πολιτικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών των σχετικών οντοτήτων, η οποία μπορεί να ενσωματωθεί σε άλλες πειθαρχικές διαδικασίες που θεσπίζονται από τις σχετικές οντότητες. Η επαλήθευση του ιστορικού των υπαλλήλων και, όπου αρμόζει, των άμεσων προμηθευτών και παρόχων υπηρεσιών των σχετικών οντοτήτων θα πρέπει να συμβάλλει στον στόχο της ασφάλειας ανθρώπινων πόρων στις σχετικές οντότητες και μπορεί να περιλαμβάνει μέτρα όπως ο έλεγχος του ποινικού μητρώου ή των προηγούμενων επαγγελματικών καθηκόντων του προσώπου, ανάλογα με την περίπτωση, όσον αφορά τα καθήκοντα του προσώπου στη σχετική οντότητα και σύμφωνα με την πολιτική της σχετικής οντότητας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

([2]) 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 (ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Η πολυπαραγοντική επαλήθευση ταυτότητας μπορεί να ενισχύσει την κυβερνοασφάλεια των οντοτήτων και θα πρέπει να εξετάζεται από τις οντότητες, ιδίως όταν οι χρήστες έχουν πρόσβαση σε συστήματα δικτύου και πληροφοριών από απομακρυσμένες τοποθεσίες ή όταν έχουν πρόσβαση σε ευαίσθητες πληροφορίες ή σε προνομιακούς λογαριασμούς και λογαριασμούς διαχείρισης συστήματος. Η πολυπαραγοντική επαλήθευση ταυτότητας μπορεί να συνδυαστεί με άλλες τεχνικές που απαιτούν πρόσθετους παράγοντες σε συγκεκριμένες περιστάσεις, βάσει προκαθορισμένων κανόνων και προτύπων, όπως η πρόσβαση από ασυνήθη τοποθεσία ή συσκευή ή σε ασυνήθη χρονική στιγμή.

(24) Οι σχετικές οντότητες θα πρέπει να διαχειρίζονται και να προστατεύουν τα πάγια στοιχεία που έχουν αξία για αυτές με γνώμονα τη χρηστή διαχείριση πάγιων στοιχείων, η οποία θα πρέπει επίσης να χρησιμεύει ως βάση για την ανάλυση κινδύνου και τη διαχείριση της επιχειρησιακής συνέχειας. Οι σχετικές οντότητες θα πρέπει να διαχειρίζονται τόσο τα υλικά όσο και τα άυλα πάγια στοιχεία και να προβαίνουν σε απογραφή πάγιων στοιχείων, να συσχετίζουν τα πάγια στοιχεία με καθορισμένο επίπεδο ταξινόμησης, να χειρίζονται και να παρακολουθούν τα πάγια στοιχεία και να λαμβάνουν μέτρα για την προστασία των πάγιων στοιχείων καθ' όλη τη διάρκεια του κύκλου ζωής τους.

(25) Η διαχείριση πάγιων στοιχείων θα πρέπει να περιλαμβάνει την ταξινόμηση των πάγιων στοιχείων ανά είδος, ευαισθησία, επίπεδο κινδύνου και απαιτήσεις ασφάλειας και την εφαρμογή κατάλληλων μέτρων και ελέγχων για τη διασφάλιση της διαθεσιμότητας, της ακεραιότητας, της εμπιστευτικότητας και της αυθεντικότητάς τους. Με την ταξινόμηση των πάγιων στοιχείων ανά επίπεδο κινδύνου, οι σχετικές οντότητες θα πρέπει να είναι σε θέση να εφαρμόζουν κατάλληλα μέτρα ασφάλειας και ελέγχους για την προστασία πάγιων στοιχείων όπως η κρυπτογράφηση, ο έλεγχος πρόσβασης, συμπεριλαμβανομένων της περιμέτρου ασφαλείας και του ελέγχου φυσικής και λογικής πρόσβασης, τα αντίγραφα ασφαλείας, η καταγραφή και η παρακολούθηση, η διατήρηση και η διάθεση. Κατά τη διενέργεια ανάλυσης επιχειρηματικών επιπτώσεων, οι σχετικές οντότητες μπορούν να καθορίζουν το επίπεδο ταξινόμησης με βάση τις συνέπειες των διαταράξεων των πάγιων στοιχείων για τις οντότητες. Όλοι οι υπάλληλοι των οντοτήτων που χειρίζονται πάγια στοιχεία θα πρέπει να είναι εξοικειωμένοι με τις πολιτικές και τις οδηγίες διαχείρισης πάγιων στοιχείων.

(26) Ο βαθμός λεπτομέρειας της απογραφής πάγιων στοιχείων θα πρέπει να είναι κατάλληλος για τις ανάγκες των σχετικών οντοτήτων. Μια ολοκληρωμένη απογραφή πάγιων στοιχείων θα μπορούσε να περιλαμβάνει, για κάθε πάγιο στοιχείο, τουλάχιστον έναν μοναδικό αναγνωριστικό κωδικό, τον ιδιοκτήτη του πάγιου στοιχείου, την περιγραφή του πάγιου στοιχείου, την τοποθεσία του πάγιου στοιχείου, το είδος του πάγιου στοιχείου, το είδος και την ταξινόμηση των πληροφοριών που υποβάλλονται σε επεξεργασία στο πάγιο στοιχείο, την ημερομηνία της τελευταίας επικαιροποίησης ή διόρθωσης του πάγιου στοιχείου, την ταξινόμηση του πάγιου στοιχείου στο πλαίσιο της εκτίμησης κινδύνου και το τέλος του κύκλου ζωής του πάγιου στοιχείου. Κατά τον προσδιορισμό του ιδιοκτήτη ενός πάγιου στοιχείου, οι σχετικές οντότητες θα πρέπει επίσης να προσδιορίζουν το πρόσωπο που είναι υπεύθυνο για την προστασία του εν λόγω πάγιου στοιχείου.

(27) Η κατανομή και η οργάνωση των ρόλων, των αρμοδιοτήτων και των εξουσιών στον τομέα της κυβερνοασφάλειας θα πρέπει να επιτρέπουν τη θέσπιση μιας συνεκτικής δομής για τη διακυβέρνηση και την εφαρμογή της κυβερνοασφάλειας εντός των σχετικών οντοτήτων, και θα πρέπει να διασφαλίζουν την αποτελεσματική επικοινωνία σε περίπτωση περιστατικών. Κατά τον καθορισμό και την ανάθεση αρμοδιοτήτων για ορισμένους ρόλους, οι σχετικές οντότητες θα πρέπει να λαμβάνουν υπόψη ρόλους όπως ο προϊστάμενος υπεύθυνος ασφάλειας πληροφοριών, ο υπεύθυνος ασφάλειας πληροφοριών, ο υπεύθυνος διαχείρισης περιστατικών, ο ελεγκτής ή ανάλογοι ισοδύναμοι ρόλοι. Οι σχετικές οντότητες μπορούν να αναθέτουν ρόλους και αρμοδιότητες σε εξωτερικά μέρη, όπως σε τρίτους παρόχους υπηρεσιών ΤΠΕ.

(28) Σύμφωνα με το άρθρο 21 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555, τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας πρέπει να βασίζονται σε μια ολική προσέγγιση των κινδύνων, η οποία να αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά όπως κλοπή, πυρκαγιά, πλημμύρες, αστοχίες στις τηλεπικοινωνίες ή στην ηλεκτροδότηση, ή μη εξουσιοδοτημένη φυσική πρόσβαση, καταστροφή και παρέμβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών της βασικής ή σημαντικής οντότητας, οι οποίες θα μπορούσαν να θέσουν σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύου και πληροφοριών. Συνεπώς, οι τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας θα πρέπει επίσης να αφορούν τη φυσική και περιβαλλοντική ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβάνοντας μέτρα για την προστασία των εν λόγω συστημάτων από αστοχίες του συστήματος, ανθρώπινα σφάλματα, κακόβουλες πράξεις ή φυσικά φαινόμενα. Άλλα παραδείγματα φυσικών και περιβαλλοντικών απειλών μπορεί να περιλαμβάνουν σεισμούς, εκρήξεις, δολιοφθορά, απειλές εκ των έσω, κοινωνικές αναταραχές, τοξικά απόβλητα και περιβαλλοντικές εκπομπές. Η πρόληψη της απώλειας, της ζημίας ή της παραβίασης των συστημάτων δικτύου και πληροφοριών ή της διακοπής της λειτουργίας τους λόγω αστοχίας και διατάραξης των υποστηρικτικών υπηρεσιών κοινής ωφελείας θα πρέπει να συμβάλλει στην επίτευξη του στόχου της επιχειρησιακής συνέχειας στις σχετικές οντότητες. Επιπλέον, η προστασία από φυσικές και περιβαλλοντικές απειλές θα πρέπει να συμβάλλει στην ασφάλεια της συντήρησης των συστημάτων δικτύου και πληροφοριών στις σχετικές οντότητες.

(29) Οι σχετικές οντότητες θα πρέπει να σχεδιάζουν και εφαρμόζουν μέτρα προστασίας από φυσικές και περιβαλλοντικές απειλές, να καθορίζουν ελάχιστα και μέγιστα όρια ελέγχου για τις φυσικές και τις περιβαλλοντικές απειλές και να παρακολουθούν τις περιβαλλοντικές παραμέτρους. Για παράδειγμα, θα πρέπει να εξετάσουν το ενδεχόμενο εγκατάστασης συστημάτων για τον εντοπισμό, σε πρώιμο στάδιο, των πλημμυρών σε περιοχές όπου βρίσκονται συστήματα δικτύου και πληροφοριών. Όσον αφορά τον κίνδυνο πυρκαγιάς, οι σχετικές οντότητες θα πρέπει να εξετάσουν το ενδεχόμενο δημιουργίας χωριστού πυροδιαμερίσματος για το κέντρο δεδομένων, τη χρήση πυράντοχων υλικών, αισθητήρων για την παρακολούθηση της θερμοκρασίας και της υγρασίας, τη σύνδεση του κτιρίου με σύστημα συναγερμού πυρκαγιάς με αυτόματη κοινοποίηση στην τοπική πυροσβεστική υπηρεσία, καθώς και συστήματα έγκαιρης πυρανίχνευσης και πυρόσβεσης. Οι σχετικές οντότητες θα πρέπει επίσης να διενεργούν τακτικές ασκήσεις πυρόσβεσης και επιθεωρήσεις πυρασφάλειας. Επιπλέον, για να διασφαλιστεί η παροχή ηλεκτρικής ενέργειας, οι σχετικές οντότητες θα πρέπει να εξετάζουν το ενδεχόμενο προστασίας από υπερτάσεις και την αντίστοιχη παροχή ηλεκτρικής ενέργειας έκτακτης ανάγκης, σύμφωνα με τα σχετικά πρότυπα. Επιπλέον, δεδομένου ότι η υπερθέρμανση ενέχει κίνδυνο για τη διαθεσιμότητα συστημάτων δικτύου και πληροφοριών, οι σχετικές οντότητες, ιδίως οι πάροχοι υπηρεσιών κέντρων δεδομένων, θα μπορούσαν να εξετάσουν κατάλληλα, συνεχή και εφεδρικά συστήματα κλιματισμού.

(30) Ο παρών κανονισμός προσδιορίζει περαιτέρω τις περιπτώσεις στις οποίες ένα περιστατικό θα πρέπει να θεωρείται σημαντικό για τους σκοπούς του άρθρου 23 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555. Τα κριτήρια θα πρέπει να είναι τέτοια ώστε οι σχετικές οντότητες να είναι σε θέση να αξιολογούν κατά πόσον ένα περιστατικό είναι σημαντικό, προκειμένου να κοινοποιούν το περιστατικό σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Επιπλέον, τα κριτήρια που καθορίζονται στον παρόντα κανονισμό θα πρέπει να θεωρούνται εξαντλητικά, με την επιφύλαξη του άρθρου 5 της οδηγίας (ΕΕ) 2022/2555. Ο παρών κανονισμός προσδιορίζει τις περιπτώσεις στις οποίες ένα περιστατικό θα πρέπει να θεωρείται σημαντικό, καθορίζοντας τόσο οριζόντιες όσο και ειδικές ανά οντότητα περιπτώσεις.

(31) Σύμφωνα με το άρθρο 23 παράγραφος 4 της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θα πρέπει να υποχρεούνται να κοινοποιούν σημαντικά περιστατικά εντός των προθεσμιών που ορίζονται στην εν λόγω διάταξη. Οι εν λόγω προθεσμίες κοινοποίησης αρχίζουν από τη στιγμή που η οντότητα λαμβάνει γνώση τέτοιων σημαντικών περιστατικών. Ως εκ τούτου, η σχετική οντότητα υποχρεούται να αναφέρει περιστατικά τα οποία, βάσει της αρχικής της αξιολόγησης, θα μπορούσαν να προκαλέσουν σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία στην εν λόγω οντότητα ή να επηρεάσουν άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία. Ως εκ τούτου, όταν μια σχετική οντότητα έχει εντοπίσει ένα ύποπτο συμβάν ή αφού ένα πιθανό περιστατικό τεθεί υπόψη της από τρίτο μέρος, όπως φυσικό πρόσωπο, πελάτης, οντότητα, αρχή, οργανισμός μέσων ενημέρωσης ή άλλη πηγή, η σχετική οντότητα θα πρέπει να αξιολογήσει εγκαίρως το ύποπτο συμβάν για να προσδιορίσει κατά πόσον συνιστά περιστατικό και, εφόσον κάτι τέτοιο διαπιστωθεί, να προσδιορίσει τη φύση και τη σοβαρότητά του. Ως εκ τούτου, η σχετική οντότητα πρέπει να θεωρείται ότι έχει λάβει «γνώση» του σημαντικού περιστατικού όταν, μετά την εν λόγω αρχική αξιολόγηση, η εν λόγω οντότητα έχει εύλογο βαθμό βεβαιότητας ότι έχει εκδηλωθεί σημαντικό περιστατικό.

(32) Προκειμένου να διαπιστωθεί αν ένα περιστατικό είναι σημαντικό, κατά περίπτωση, οι σχετικές οντότητες θα πρέπει να υπολογίζουν τον αριθμό των χρηστών που επηρεάζονται από το περιστατικό, λαμβάνοντας υπόψη τους επιχειρηματικούς και τελικούς πελάτες με τους οποίους οι σχετικές οντότητες έχουν συμβατική σχέση, καθώς και τα φυσικά και νομικά πρόσωπα που συνδέονται με επιχειρηματικούς πελάτες. Όταν μια σχετική οντότητα δεν είναι σε θέση να υπολογίσει τον αριθμό των επηρεαζόμενων χρηστών, η εκτίμηση της σχετικής οντότητας για τον πιθανό μέγιστο αριθμό επηρεαζόμενων χρηστών θα πρέπει να λαμβάνεται υπόψη για τον υπολογισμό του συνολικού αριθμού των χρηστών που επηρεάζονται από το περιστατικό. Η σημασία ενός περιστατικού που αφορά υπηρεσία εμπιστοσύνης θα πρέπει να καθορίζεται όχι μόνο από τον αριθμό των χρηστών, αλλά και από τον αριθμό των βασιζόμενων μερών, καθώς αυτά μπορούν να επηρεαστούν εξίσου από σημαντικό περιστατικό που αφορά υπηρεσία εμπιστοσύνης όσον αφορά λειτουργική διατάραξη και υλική ή μη υλική ζημία. Ως εκ τούτου, οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει, όπου αρμόζει, να λαμβάνουν επίσης υπόψη τον αριθμό των βασιζόμενων μερών κατά τον προσδιορισμό του κατά πόσον ένα περιστατικό είναι σημαντικό. Για τον σκοπό αυτό, ως βασιζόμενα μέρη θα πρέπει να νοούνται τα φυσικά ή νομικά πρόσωπα που βασίζονται σε υπηρεσία εμπιστοσύνης.

(33) Οι εργασίες συντήρησης που έχουν ως αποτέλεσμα την περιορισμένη διαθεσιμότητα ή τη μη διαθεσιμότητα των υπηρεσιών δεν θα πρέπει να θεωρούνται σημαντικά περιστατικά εάν η περιορισμένη διαθεσιμότητα ή η μη διαθεσιμότητα της υπηρεσίας προκύπτει σύμφωνα με προγραμματισμένη εργασία συντήρησης. Επιπλέον, όταν μια υπηρεσία είναι μη διαθέσιμη λόγω προγραμματισμένων διακοπών, όπως διακοπών ή μη διαθεσιμότητας βάσει προκαθορισμένης συμβατικής συμφωνίας, δεν θα πρέπει να θεωρείται σημαντικό περιστατικό.

(34) Η διάρκεια ενός περιστατικού που επηρεάζει τη διαθεσιμότητα μιας υπηρεσίας θα πρέπει να μετράται από τη διακοπή της ορθής παροχής της εν λόγω υπηρεσίας έως τον χρόνο αποκατάστασης. Όταν μια σχετική οντότητα δεν είναι σε θέση να προσδιορίσει τη στιγμή έναρξης της διατάραξης, η διάρκεια του περιστατικού θα πρέπει να μετράται από τη στιγμή που εντοπίστηκε το περιστατικό ή από τη στιγμή κατά την οποία το περιστατικό καταγράφηκε στα αρχεία καταγραφής του δικτύου ή του συστήματος ή σε άλλες πηγές δεδομένων, ανάλογα με το ποια ημερομηνία είναι προγενέστερη.

(35) Η πλήρης μη διαθεσιμότητα μιας υπηρεσίας θα πρέπει να μετράται από τη στιγμή που η υπηρεσία είναι πλήρως μη διαθέσιμη στους χρήστες έως τη στιγμή κατά την οποία οι τακτικές δραστηριότητες ή λειτουργίες έχουν αποκατασταθεί στο επίπεδο της υπηρεσίας που παρεχόταν πριν από το περιστατικό. Όταν μια σχετική οντότητα δεν είναι σε θέση να προσδιορίσει πότε άρχισε η πλήρης μη διαθεσιμότητα μιας υπηρεσίας, η μη διαθεσιμότητα θα πρέπει να μετράται από τη στιγμή που εντοπίστηκε από την εν λόγω οντότητα.

(36) Για τον προσδιορισμό των άμεσων οικονομικών ζημιών που προκύπτουν από περιστατικό, οι σχετικές οντότητες θα πρέπει να λαμβάνουν υπόψη όλες τις οικονομικές ζημίες που υπέστησαν ως αποτέλεσμα του περιστατικού, όπως οι δαπάνες αντικατάστασης ή μετεγκατάστασης λογισμικού, υλισμικού ή υποδομής, οι δαπάνες προσωπικού, συμπεριλαμβανομένων των δαπανών που συνδέονται με την αντικατάσταση ή τη μετεγκατάσταση του προσωπικού, την πρόσληψη επιπλέον προσωπικού, τις αμοιβές υπερωριών και την ανάκτηση απολεσθεισών ή υποβαθμισμένων δεξιοτήτων, τα τέλη λόγω μη συμμόρφωσης με τις συμβατικές υποχρεώσεις, τα έξοδα επανόρθωσης και αποζημίωσης των πελατών, οι απώλειες λόγω διαφυγόντων εσόδων, οι δαπάνες που συνδέονται με την εσωτερική και εξωτερική επικοινωνία, οι δαπάνες παροχής συμβουλών, συμπεριλαμβανομένων των δαπανών που συνδέονται με νομικές συμβουλές, εγκληματολογικές υπηρεσίες και υπηρεσίες αποκατάστασης, και άλλες δαπάνες που συνδέονται με το περιστατικό. Ωστόσο, τα διοικητικά πρόστιμα καθώς και οι δαπάνες που είναι αναγκαίες για την καθημερινή λειτουργία της επιχείρησης δεν θα πρέπει να θεωρούνται οικονομικές ζημίες που προκύπτουν από περιστατικό, συμπεριλαμβανομένων των δαπανών για τη γενική συντήρηση της υποδομής, του εξοπλισμού, του υλισμικού και του λογισμικού, της επικαιροποίησης των δεξιοτήτων του προσωπικού, των εσωτερικών ή εξωτερικών δαπανών για την ενίσχυση της επιχείρησης μετά το περιστατικό, συμπεριλαμβανομένων των αναβαθμίσεων, των βελτιώσεων και των πρωτοβουλιών εκτίμησης κινδύνου, καθώς και των ασφαλίστρων. Οι σχετικές οντότητες θα πρέπει να υπολογίζουν τα ποσά των οικονομικών ζημιών με βάση τα διαθέσιμα δεδομένα και, όταν τα πραγματικά ποσά των οικονομικών ζημιών δεν μπορούν να προσδιοριστούν, οι οντότητες θα πρέπει να εκτιμούν τα εν λόγω ποσά.

(37) Οι σχετικές οντότητες θα πρέπει επίσης να υποχρεούνται να αναφέρουν περιστατικά που έχουν προκαλέσει ή μπορούν να προκαλέσουν τον θάνατο φυσικών προσώπων ή σημαντικές βλάβες στην υγεία των φυσικών προσώπων, καθώς τα περιστατικά αυτά αποτελούν ιδιαίτερα σοβαρές περιπτώσεις πρόκλησης σημαντικής υλικής ή μη υλικής ζημίας. Για παράδειγμα, περιστατικό που επηρεάζει σχετική οντότητα θα μπορούσε να προκαλέσει μη διαθεσιμότητα υπηρεσιών υγειονομικής περίθαλψης ή έκτακτης ανάγκης ή απώλεια της εμπιστευτικότητας ή της ακεραιότητας των δεδομένων με επιπτώσεις στην υγεία των φυσικών προσώπων. Προκειμένου να προσδιοριστεί αν ένα περιστατικό έχει προκαλέσει ή μπορεί να προκαλέσει σημαντική βλάβη στην υγεία φυσικού προσώπου, οι σχετικές οντότητες θα πρέπει να λαμβάνουν υπόψη κατά πόσον το περιστατικό προκάλεσε ή μπορεί να προκαλέσει σοβαρούς τραυματισμούς και προβλήματα υγείας. Για τον σκοπό αυτό, οι σχετικές οντότητες δεν θα πρέπει να υποχρεούνται να συλλέγουν πρόσθετες πληροφορίες στις οποίες δεν έχουν πρόσβαση.

(38) Περιορισμένη διαθεσιμότητα θα πρέπει να θεωρείται ότι υφίσταται ιδίως όταν μια υπηρεσία που παρέχεται από σχετική οντότητα είναι σημαντικά βραδύτερη από τον μέσο χρόνο απόκρισης ή όταν δεν είναι διαθέσιμες όλες οι λειτουργίες μιας υπηρεσίας. Όπου είναι δυνατόν, θα πρέπει να χρησιμοποιούνται αντικειμενικά κριτήρια με βάση τον μέσο χρόνο απόκρισης των υπηρεσιών που παρέχονται από τις σχετικές οντότητες για την αξιολόγηση των καθυστερήσεων στον χρόνο απόκρισης. Λειτουργία μιας υπηρεσίας μπορεί να αποτελεί, για παράδειγμα, μια λειτουργία συνομιλίας ή μια λειτουργία αναζήτησης εικόνων.

(39) Η επιτυχής, ύποπτα κακόβουλη και μη εξουσιοδοτημένη πρόσβαση στα συστήματα δικτύου και πληροφοριών μιας σχετικής οντότητας θα πρέπει να θεωρείται σημαντικό περιστατικό, όταν η πρόσβαση αυτή είναι ικανή να προκαλέσει σοβαρή λειτουργική διατάραξη. Για παράδειγμα, όταν ένας παράγοντας κυβερνοαπειλής τοποθετείται εκ των προτέρων στα συστήματα δικτύου και πληροφοριών μιας σχετικής οντότητας με σκοπό την πρόκληση διατάραξης των υπηρεσιών στο μέλλον, το περιστατικό θα πρέπει να θεωρείται σημαντικό.

(40) Τα επαναλαμβανόμενα περιστατικά που συνδέονται με την ίδια προφανή βαθύτερη αιτία, τα οποία μεμονωμένα δεν πληρούν τα κριτήρια ενός σημαντικού περιστατικού, θα πρέπει συλλογικά να θεωρούνται σημαντικό περιστατικό, υπό την προϋπόθεση ότι πληρούν συλλογικά το κριτήριο της οικονομικής ζημίας και ότι έχουν εκδηλωθεί τουλάχιστον δύο φορές εντός έξι μηνών. Τα εν λόγω επαναλαμβανόμενα περιστατικά μπορούν να υποδεικνύουν σημαντικές ελλείψεις και αδυναμίες, αφενός, στις διαδικασίες της σχετικής οντότητας όσον αφορά τη διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και, αφετέρου, στο επίπεδο ωριμότητάς τους στον τομέα της κυβερνοασφάλειας. Επιπλέον, τέτοια επαναλαμβανόμενα περιστατικά είναι ικανά να προκαλέσουν σημαντική οικονομική ζημία στη σχετική οντότητα.

(41) Η Επιτροπή αντάλλαξε συμβουλές και συνεργάστηκε με την Ομάδα Συνεργασίας και τον ENISA σχετικά με το σχέδιο εκτελεστικής πράξης, σύμφωνα με το άρθρο 21 παράγραφος 5 και το άρθρο 23 παράγραφος 11 της οδηγίας (ΕΕ) 2022/2555.

(42) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε την 1η Σεπτεμβρίου 2024.

(43) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί δυνάμει του άρθρου 39 της οδηγίας (ΕΕ) 2022/2555,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Αντικείμενο

Ο παρών κανονισμός, όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης (στο εξής: σχετικές οντότητες), καθορίζει τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων που αναφέρονται στο άρθρο 21 παράγραφος 2 της οδηγίας (ΕΕ) 2022/2555 και προσδιορίζει περαιτέρω τις περιπτώσεις στις οποίες ένα περιστατικό θεωρείται σημαντικό, όπως αναφέρεται στο άρθρο 23 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555.

Άρθρο 2

Τεχνικές και μεθοδολογικές απαιτήσεις

1. Για τις σχετικές οντότητες, οι τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που αναφέρονται στο άρθρο 21 παράγραφος 2 στοιχεία α) έως ι) της οδηγίας (ΕΕ) 2022/2555 ορίζονται στο παράρτημα του παρόντος κανονισμού.

2. Οι σχετικές οντότητες διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών κατάλληλο για τους κινδύνους που ενέχουν κατά την υλοποίηση και την εφαρμογή των τεχνικών και μεθοδολογικών απαιτήσεων των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού. Για τον σκοπό αυτό, λαμβάνουν δεόντως υπόψη τον βαθμό έκθεσής τους σε κινδύνους, το μέγεθός τους και την πιθανότητα εμφάνισης περιστατικών και τη σοβαρότητά τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεών τους, κατά τη συμμόρφωση με τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ορίζονται στο παράρτημα του παρόντος κανονισμού.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Όταν το παράρτημα του παρόντος κανονισμού προβλέπει ότι μια τεχνική ή μεθοδολογική απαίτηση ενός μέτρου διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας εφαρμόζεται «κατά περίπτωση», «όπου αρμόζει» ή «στον βαθμό που αυτό είναι εφικτό», και όταν μια σχετική οντότητα θεωρεί ότι δεν είναι κατάλληλο, δεν είναι σκόπιμο ή δεν είναι εφικτό για τη σχετική οντότητα να εφαρμόσει ορισμένες τέτοιες τεχνικές και μεθοδολογικές απαιτήσεις, η σχετική οντότητα τεκμηριώνει με κατανοητό τρόπο το σκεπτικό της για τον σκοπό αυτό.

Άρθρο 3

Σημαντικά περιστατικά

1. Ένα περιστατικό θεωρείται σημαντικό για τους σκοπούς του άρθρου 23 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις σχετικές οντότητες όταν πληρούνται ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) το περιστατικό έχει προκαλέσει ή μπορεί να προκαλέσει άμεση οικονομική ζημία για τη σχετική οντότητα που υπερβαίνει τα 500 000 EUR ή το 5 % του συνολικού ετήσιου κύκλου εργασιών της σχετικής οντότητας κατά το προηγούμενο οικονομικό έτος, όποιο από τα δύο ποσά είναι χαμηλότερο·

β) το περιστατικό έχει προκαλέσει ή μπορεί να προκαλέσει την απόσπαση εμπορικών απορρήτων της σχετικής οντότητας, όπως ορίζονται στο άρθρο 2 σημείο 1 της οδηγίας (ΕΕ) 2016/943·

γ) το περιστατικό έχει προκαλέσει ή μπορεί να προκαλέσει τον θάνατο φυσικού προσώπου·

δ) το περιστατικό έχει προκαλέσει ή μπορεί να προκαλέσει σημαντική βλάβη στην υγεία φυσικού προσώπου·

ε) υπήρξε επιτυχής, ύποπτα κακόβουλη και μη εξουσιοδοτημένη πρόσβαση σε συστήματα δικτύου και πληροφοριών, η οποία μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη·

στ) το περιστατικό πληροί τα κριτήρια που ορίζονται στο άρθρο 4·

ζ) το περιστατικό πληροί ένα ή περισσότερα από τα κριτήρια που ορίζονται στα άρθρα 5 έως 14.

2. Οι προγραμματισμένες διακοπές της υπηρεσίας και οι αναμενόμενες συνέπειες των προγραμματισμένων εργασιών συντήρησης που εκτελούνται από τις σχετικές οντότητες ή για λογαριασμό τους δεν θεωρούνται σημαντικά περιστατικά.

3. Κατά τον υπολογισμό του αριθμού των χρηστών που επηρεάζονται από περιστατικό για τους σκοπούς των άρθρων 7 και 9 έως 14, οι σχετικές οντότητες λαμβάνουν υπόψη όλα τα ακόλουθα:

α) τον αριθμό των πελατών που έχουν σύμβαση με τη σχετική οντότητα η οποία τους παρέχει πρόσβαση στα συστήματα δικτύου και πληροφοριών της σχετικής οντότητας ή στις υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών·

β) τον αριθμό των φυσικών και νομικών προσώπων που συνδέονται με επιχειρηματικούς πελάτες που χρησιμοποιούν τα συστήματα δικτύου και πληροφοριών των οντοτήτων ή τις υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών.

Άρθρο 4

Επαναλαμβανόμενα περιστατικά

Τα περιστατικά που μεμονωμένα δεν θεωρούνται σημαντικό περιστατικό κατά την έννοια του άρθρου 3 θεωρούνται συλλογικά ως ένα σημαντικό περιστατικό όταν πληρούν όλα τα ακόλουθα κριτήρια:

α) έχουν εκδηλωθεί τουλάχιστον δύο φορές εντός 6 μηνών·

β) έχουν την ίδια προφανή βαθύτερη αιτία·

γ) πληρούν συλλογικά τα κριτήρια που ορίζονται στο άρθρο 3 παράγραφος 1 στοιχείο α).

Άρθρο 5

Σημαντικά περιστατικά όσον αφορά τους παρόχους υπηρεσιών DNS

Όσον αφορά τους παρόχους υπηρεσιών DNS, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια υπηρεσία επαναλαμβανόμενης ή έγκυρης επίλυσης ονομάτων τομέα είναι πλήρως μη διαθέσιμη για περισσότερα από 30 λεπτά·

β) για χρονικό διάστημα μεγαλύτερο της μίας ώρας, ο μέσος χρόνος απόκρισης μιας υπηρεσίας επαναλαμβανόμενης ή έγκυρης επίλυσης ονομάτων τομέα σε αιτήματα DNS υπερβαίνει τα 10 δευτερόλεπτα·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή της υπηρεσίας έγκυρης επίλυσης ονομάτων τομέα, εκτός από τις περιπτώσεις όπου τα δεδομένα λιγότερων από 1 000 ονομάτων τομέα που διαχειρίζεται ο πάροχος υπηρεσιών DNS, τα οποία δεν υπερβαίνουν το 1 % των ονομάτων τομέα που διαχειρίζεται ο πάροχος υπηρεσιών DNS, δεν είναι ορθά λόγω εσφαλμένης παραμετροποίησης.

Άρθρο 6

Σημαντικά περιστατικά όσον αφορά τα μητρώα ονομάτων TLD

Όσον αφορά τα μητρώα ονομάτων TLD, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια υπηρεσία έγκυρης επίλυσης ονομάτων τομέα είναι πλήρως μη διαθέσιμη·

β) για χρονικό διάστημα μεγαλύτερο της μίας ώρας, ο μέσος χρόνος απόκρισης μιας υπηρεσίας έγκυρης επίλυσης ονομάτων τομέα σε αιτήματα DNS υπερβαίνει τα 10 δευτερόλεπτα·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την τεχνική λειτουργία του TLD.

Άρθρο 7

Σημαντικά περιστατικά όσον αφορά τους παρόχους υπηρεσιών υπολογιστικού νέφους

Όσον αφορά τους παρόχους υπηρεσιών υπολογιστικού νέφους, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μία παρεχόμενη υπηρεσία υπολογιστικού νέφους είναι πλήρως μη διαθέσιμη για περισσότερα από 30 λεπτά·

β) η διαθεσιμότητα μιας υπηρεσίας υπολογιστικού νέφους ενός παρόχου είναι περιορισμένη για περισσότερο από το 5 % των χρηστών της υπηρεσίας υπολογιστικού νέφους στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες της υπηρεσίας υπολογιστικού νέφους στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, για διάρκεια μεγαλύτερη της μίας ώρας·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας υπηρεσίας υπολογιστικού νέφους ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας υπηρεσίας υπολογιστικού νέφους με αντίκτυπο σε περισσότερο από το 5 % των χρηστών της εν λόγω υπηρεσίας υπολογιστικού νέφους στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω υπηρεσίας υπολογιστικού νέφους στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 8

Σημαντικά περιστατικά όσον αφορά τους παρόχους υπηρεσιών κέντρων δεδομένων

Όσον αφορά τους παρόχους υπηρεσιών κέντρων δεδομένων, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) η υπηρεσία κέντρου δεδομένων ενός κέντρου δεδομένων που διαχειρίζεται ο πάροχος είναι πλήρως μη διαθέσιμη·

β) η διαθεσιμότητα μιας υπηρεσίας κέντρου δεδομένων ενός κέντρου δεδομένων που διαχειρίζεται ο πάροχος είναι περιορισμένη για διάρκεια μεγαλύτερη της μίας ώρας·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας υπηρεσίας κέντρου δεδομένων ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η φυσική πρόσβαση σε ένα κέντρο δεδομένων που διαχειρίζεται ο πάροχος.

Άρθρο 9

Σημαντικά περιστατικά όσον αφορά τους παρόχους δικτύων διανομής περιεχομένου

Όσον αφορά τους παρόχους δικτύων διανομής περιεχομένου, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) ένα δίκτυο διανομής περιεχομένου είναι πλήρως μη διαθέσιμο για περισσότερα από 30 λεπτά·

β) η διαθεσιμότητα ενός δικτύου διανομής περιεχομένου είναι περιορισμένη για περισσότερο από το 5 % των χρηστών του δικτύου διανομής περιεχομένου στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες του δικτύου διανομής περιεχομένου στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, για διάρκεια μεγαλύτερη της μίας ώρας·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή ενός δικτύου διανομής περιεχομένου ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή ενός δικτύου διανομής περιεχομένου με αντίκτυπο σε περισσότερο από το 5 % των χρηστών του εν λόγω δικτύου διανομής περιεχομένου στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες του εν λόγω δικτύου διανομής περιεχομένου στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 10

Σημαντικά περιστατικά όσον αφορά τους παρόχους διαχειριζόμενων υπηρεσιών και τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας

Όσον αφορά τους παρόχους διαχειριζόμενων υπηρεσιών και τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια διαχειριζόμενη υπηρεσία ή διαχειριζόμενη υπηρεσία ασφάλειας είναι πλήρως μη διαθέσιμη για περισσότερα από 30 λεπτά·

β) η διαθεσιμότητα μιας διαχειριζόμενης υπηρεσίας ή μιας διαχειριζόμενης υπηρεσίας ασφάλειας είναι περιορισμένη για περισσότερο από το 5 % των χρηστών της υπηρεσίας στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες της υπηρεσίας στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, για διάρκεια μεγαλύτερη της μίας ώρας·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας διαχειριζόμενης υπηρεσίας ή διαχειριζόμενης υπηρεσίας ασφάλειας ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας διαχειριζόμενης υπηρεσίας ή μιας διαχειριζόμενης υπηρεσίας ασφάλειας με αντίκτυπο σε περισσότερο από το 5 % των χρηστών της εν λόγω διαχειριζόμενης υπηρεσίας ή της εν λόγω διαχειριζόμενης υπηρεσίας ασφάλειας στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες της υπηρεσίας στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 11

Σημαντικά περιστατικά όσον αφορά τους παρόχους επιγραμμικών αγορών

Όσον αφορά τους παρόχους επιγραμμικών αγορών, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια επιγραμμική αγορά είναι πλήρως μη διαθέσιμη για περισσότερο από το 5 % των χρηστών μιας επιγραμμικής αγοράς στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες μιας επιγραμμικής αγοράς στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος·

β) περισσότερο από το 5 % των χρηστών μιας επιγραμμικής αγοράς στην Ένωση ή περισσότεροι από 1 εκατομμύριο χρήστες μιας επιγραμμικής αγοράς στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, επηρεάζονται από την περιορισμένη διαθεσιμότητα της εν λόγω επιγραμμικής αγοράς·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας επιγραμμικής αγοράς ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας επιγραμμικής αγοράς με αντίκτυπο σε περισσότερο από το 5 % των χρηστών της εν λόγω επιγραμμικής αγοράς στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω επιγραμμικής αγοράς στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 12

Σημαντικά περιστατικά όσον αφορά τους παρόχους επιγραμμικών μηχανών αναζήτησης

Όσον αφορά τους παρόχους επιγραμμικών μηχανών αναζήτησης, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια επιγραμμική μηχανή αναζήτησης είναι πλήρως μη διαθέσιμη για περισσότερο από το 5 % των χρηστών της εν λόγω επιγραμμικής μηχανής αναζήτησης στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω επιγραμμικής μηχανής αναζήτησης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος·

β) περισσότερο από το 5 % των χρηστών μιας επιγραμμικής μηχανής αναζήτησης στην Ένωση ή περισσότεροι από 1 εκατομμύριο χρήστες μιας επιγραμμικής μηχανής αναζήτησης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, επηρεάζονται από την περιορισμένη διαθεσιμότητα της εν λόγω επιγραμμικής μηχανής αναζήτησης·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας επιγραμμικής μηχανής αναζήτησης ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας επιγραμμικής μηχανής αναζήτησης με αντίκτυπο σε περισσότερο από το 5 % των χρηστών της εν λόγω επιγραμμικής μηχανής αναζήτησης στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω επιγραμμικής μηχανής αναζήτησης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 13

Σημαντικά περιστατικά όσον αφορά τους παρόχους πλατφορμών υπηρεσιών κοινωνικής δικτύωσης

Όσον αφορά τους παρόχους πλατφορμών υπηρεσιών κοινωνικής δικτύωσης, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μια πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης είναι πλήρως μη διαθέσιμη για περισσότερο από το 5 % των χρηστών της εν λόγω πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση ή για περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος·

β) περισσότερο από το 5 % των χρηστών μιας πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση ή περισσότεροι από 1 εκατομμύριο χρήστες μιας πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, επηρεάζονται από την περιορισμένη διαθεσιμότητα της εν λόγω πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης·

γ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης ως αποτέλεσμα ύποπτα κακόβουλης ενέργειας·

δ) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης με αντίκτυπο σε περισσότερο από το 5 % των χρηστών της εν λόγω πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση ή σε περισσότερους από 1 εκατομμύριο χρήστες της εν λόγω πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 14

Σημαντικά περιστατικά όσον αφορά τους παρόχους υπηρεσιών εμπιστοσύνης

Όσον αφορά τους παρόχους υπηρεσιών εμπιστοσύνης, ένα περιστατικό θεωρείται σημαντικό σύμφωνα με το άρθρο 3 παράγραφος 1 στοιχείο ζ), όταν πληροί ένα ή περισσότερα από τα ακόλουθα κριτήρια:

α) μία υπηρεσία εμπιστοσύνης είναι πλήρως μη διαθέσιμη για περισσότερα από 20 λεπτά·

β) μια υπηρεσία εμπιστοσύνης είναι μη διαθέσιμη στους χρήστες ή στα βασιζόμενα μέρη για διάρκεια μεγαλύτερη της μίας ώρας, η οποία υπολογίζεται ανά ημερολογιακή εβδομάδα·

γ) περισσότερο από το 1 % των χρηστών ή των βασιζόμενων μερών στην Ένωση ή περισσότεροι από 200 000 χρήστες ή βασιζόμενα μέρη στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος, επηρεάζονται από την περιορισμένη διαθεσιμότητα μιας υπηρεσίας εμπιστοσύνης·

δ) διακυβεύεται η φυσική πρόσβαση σε περιοχή όπου βρίσκονται συστήματα δικτύου και πληροφοριών και στην οποία η πρόσβαση περιορίζεται σε αξιόπιστο προσωπικό του παρόχου υπηρεσιών εμπιστοσύνης, ή η προστασία της εν λόγω φυσικής πρόσβασης·

ε) διακυβεύεται η ακεραιότητα, η εμπιστευτικότητα ή η αυθεντικότητα των αποθηκευμένων, διαβιβαζόμενων ή υφιστάμενων επεξεργασία δεδομένων που σχετίζονται με την παροχή μιας υπηρεσίας εμπιστοσύνης με αντίκτυπο σε περισσότερο από το 0,1 % των χρηστών ή των βασιζόμενων μερών, ή σε περισσότερους από 100 χρήστες ή βασιζόμενα μέρη της υπηρεσίας εμπιστοσύνης στην Ένωση, όποιος από τους δύο αριθμούς είναι μικρότερος.

Άρθρο 15

Κατάργηση

Ο εκτελεστικός κανονισμός (ΕΕ) 2018/151 της Επιτροπής ([4]) καταργείται.

Άρθρο 16

Έναρξη ισχύος και εφαρμογή

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, 17 Οκτωβρίου 2024.

Για την Επιτροπή
Ursula VON DER LEYEN
Η Πρόεδρος

([4]) Εκτελεστικός κανονισμός (ΕΕ) 2018/151 της Επιτροπής, της 30ής Ιανουαρίου 2018, που θεσπίζει κανόνες για την εφαρμογή της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, όσον αφορά τον περαιτέρω προσδιορισμό των στοιχείων που πρέπει να λαμβάνονται υπόψη από τους παρόχους ψηφιακών υπηρεσιών για τη διαχείριση κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών, καθώς και των παραμέτρων βάσει των οποίων καθορίζεται κατά πόσον ο αντίκτυπος συμβάντος είναι σημαντικός (ΕΕ L 26 της 31.1.2018, σ. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

ΠΑΡΑΡΤΗΜΑ

Τεχνικές και μεθοδολογικές απαιτήσεις που αναφέρονται στο άρθρο 2 του παρόντος κανονισμού

1. **Πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών [άρθρο 21 παράγραφος 2 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555]**

1.1. *Πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών*

1.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555, η πολιτική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών:

α) καθορίζει την προσέγγιση των σχετικών οντοτήτων όσον αφορά τη διαχείριση της ασφάλειας των οικείων συστημάτων δικτύου και πληροφοριών·

β) είναι κατάλληλη και συμπληρωματική προς την επιχειρηματική στρατηγική και τους στόχους των σχετικών οντοτήτων·

γ) καθορίζει στόχους για την ασφάλεια δικτύου και πληροφοριών·

δ) περιλαμβάνει δέσμευση για συνεχή βελτίωση της ασφάλειας των συστημάτων δικτύου και πληροφοριών·

ε) περιλαμβάνει δέσμευση για την παροχή των κατάλληλων πόρων που απαιτούνται για την εφαρμογή της, συμπεριλαμβανομένων του απαραίτητου προσωπικού, των οικονομικών πόρων, των διαδικασιών, των εργαλείων και των τεχνολογιών που απαιτούνται·

στ) κοινοποιείται και αναγνωρίζεται από τους σχετικούς υπαλλήλους και τα σχετικά ενδιαφερόμενα εξωτερικά μέρη·

ζ) καθορίζει τους ρόλους και τις αρμοδιότητες σύμφωνα με το σημείο 1.2.·

η) απαριθμεί τα έγγραφα που πρέπει να τηρούνται και τη διάρκεια διατήρησης των εγγράφων·

θ) απαριθμεί τις πολιτικές για συγκεκριμένα θέματα·

ι) καθορίζει δείκτες και μέτρα για την παρακολούθηση της εφαρμογής της και της τρέχουσας κατάστασης του επιπέδου ωριμότητας της ασφάλειας δικτύου και πληροφοριών των σχετικών οντοτήτων·

ια) αναφέρει την ημερομηνία της επίσημης έγκρισης από τα διοικητικά όργανα των σχετικών οντοτήτων (στο εξής: διοικητικά όργανα).

1.1.2. Η πολιτική για την ασφάλεια συστημάτων δικτύου και πληροφοριών αξιολογείται και, κατά περίπτωση, επικαιροποιείται από τα διοικητικά όργανα τουλάχιστον ετησίως και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους. Το αποτέλεσμα των αξιολογήσεων τεκμηριώνεται.

1.2. *Ρόλοι, αρμοδιότητες και εξουσίες*

1.2.1. Στο πλαίσιο της οικείας πολιτικής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών που αναφέρεται στο σημείο 1.1., οι σχετικές οντότητες καθορίζουν τις αρμοδιότητες και τις εξουσίες για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και τις αναθέτουν σε ρόλους, τις κατανέμουν ανάλογα με τις ανάγκες των σχετικών οντοτήτων και τις κοινοποιούν στα διοικητικά όργανα.

1.2.2. Οι σχετικές οντότητες απαιτούν από όλο το προσωπικό και τα τρίτα μέρη να εφαρμόζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών σύμφωνα με την καθιερωμένη πολιτική για την ασφάλεια δικτύου και πληροφοριών, τις πολιτικές για συγκεκριμένα θέματα και τις διαδικασίες των σχετικών οντοτήτων.

1.2.3. Τουλάχιστον ένα πρόσωπο υποβάλλει εκθέσεις απευθείας στα διοικητικά όργανα για θέματα ασφάλειας των συστημάτων δικτύου και πληροφοριών.

1.2.4. Ανάλογα με το μέγεθος των σχετικών οντοτήτων, η ασφάλεια των συστημάτων δικτύου και πληροφοριών καλύπτεται από ειδικούς ρόλους ή καθήκοντα που εκτελούνται επιπλέον των υφιστάμενων ρόλων.

1.2.5. Τα συγκρουόμενα καθήκοντα και οι συγκρουόμενοι τομείς ευθύνης διαχωρίζονται, όπου αρμόζει.

1.2.6. Οι ρόλοι, οι αρμοδιότητες και οι εξουσίες αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται από τα διοικητικά όργανα σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

2. **Πολιτική διαχείρισης κινδύνων [άρθρο 21 παράγραφος 2 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555]**

2.1. *Πλαίσιο διαχείρισης κινδύνων*

2.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο α) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν και διατηρούν κατάλληλο πλαίσιο διαχείρισης κινδύνων για τον προσδιορισμό και την αντιμετώπιση των κινδύνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Οι σχετικές οντότητες διενεργούν και τεκμηριώνουν εκτιμήσεις κινδύνου και, με βάση τα αποτελέσματα, καταρτίζουν, εφαρμόζουν και παρακολουθούν σχέδιο αντιμετώπισης κινδύνων. Τα αποτελέσματα της εκτίμησης κινδύνου και οι υπολειπόμενοι κίνδυνοι γίνονται δεκτά από τα διοικητικά όργανα ή, όπου αρμόζει, από πρόσωπα που είναι υπόλογα και έχουν την εξουσία να διαχειρίζονται τους κινδύνους, υπό την προϋπόθεση ότι οι σχετικές οντότητες διασφαλίζουν την κατάλληλη υποβολή εκθέσεων στα διοικητικά όργανα.

2.1.2. Για τους σκοπούς του σημείου 2.1.1., οι σχετικές οντότητες θεσπίζουν διαδικασίες για τον προσδιορισμό, την ανάλυση, την αξιολόγηση και την αντιμετώπιση των κινδύνων (στο εξής: διαδικασία διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας). Η διαδικασία διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας αποτελεί αναπόσπαστο μέρος της γενικότερης διαδικασίας διαχείρισης κινδύνων των σχετικών οντοτήτων, όπου αρμόζει. Στο πλαίσιο της διαδικασίας διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, οι σχετικές οντότητες:

α) ακολουθούν μεθοδολογία διαχείρισης κινδύνων·

β) καθορίζουν το επίπεδο ανοχής κινδύνου σύμφωνα με τη διάθεση ανάληψης κινδύνου των σχετικών οντοτήτων·

γ) θεσπίζουν και διατηρούν σχετικά κριτήρια κινδύνου·

δ) σύμφωνα με μια ολική προσέγγιση των κινδύνων, προσδιορίζουν και τεκμηριώνουν τους κινδύνους για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ιδίως σε σχέση με τρίτα μέρη και τους κινδύνους που θα μπορούσαν να οδηγήσουν σε διαταράξεις στη διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα και την εμπιστευτικότητα των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του προσδιορισμού μοναδικών σημείων αστοχίας·

ε) αναλύουν τους κινδύνους για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων των απειλών, των πιθανοτήτων, των επιπτώσεων και του επιπέδου κινδύνου, λαμβάνοντας υπόψη τις πληροφορίες για κυβερνοαπειλές και ευπάθειες·

στ) αξιολογούν τους προσδιορισθέντες κινδύνους με βάση τα κριτήρια κινδύνου·

ζ) προσδιορίζουν και ιεραρχούν κατάλληλες επιλογές και μέτρα αντιμετώπισης κινδύνων·

η) παρακολουθούν συνεχώς την εφαρμογή των μέτρων αντιμετώπισης των κινδύνων·

θ) προσδιορίζουν το πρόσωπο που είναι υπεύθυνο για την εφαρμογή των μέτρων αντιμετώπισης κινδύνων και τον χρόνο εφαρμογής τους·

ι) τεκμηριώνουν τα επιλεγμένα μέτρα αντιμετώπισης κινδύνων σε ένα σχέδιο αντιμετώπισης κινδύνων και τους λόγους που δικαιολογούν την αποδοχή των υπολειπόμενων κινδύνων με κατανοητό τρόπο.

2.1.3. Κατά τον προσδιορισμό και την ιεράρχηση κατάλληλων επιλογών και μέτρων όσον αφορά την αντιμετώπιση κινδύνων, οι σχετικές οντότητες λαμβάνουν υπόψη τα αποτελέσματα της εκτίμησης κινδύνου, τα αποτελέσματα της διαδικασίας για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, το κόστος εφαρμογής σε σχέση με το αναμενόμενο όφελος, την ταξινόμηση πάγιων στοιχείων που αναφέρεται στο σημείο 12.1. και την ανάλυση επιχειρηματικών επιπτώσεων που αναφέρεται στο σημείο 4.1.3.

2.1.4. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τα αποτελέσματα της εκτίμησης κινδύνου και το σχέδιο αντιμετώπισης κινδύνων σε προγραμματισμένα χρονικά διαστήματα και τουλάχιστον ετησίως, και σε περίπτωση εκδήλωσης σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους ή σημαντικών περιστατικών.

2.2. *Παρακολούθηση της συμμόρφωσης*

2.2.1. Οι σχετικές οντότητες αξιολογούν τακτικά τη συμμόρφωση με τις οικείες πολιτικές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τις πολιτικές για συγκεκριμένα θέματα, τους κανόνες και τα πρότυπα. Τα διοικητικά όργανα ενημερώνονται για την κατάσταση της ασφάλειας δικτύου και πληροφοριών βάσει των αξιολογήσεων συμμόρφωσης μέσω τακτικής υποβολής εκθέσεων.

2.2.2. Οι σχετικές οντότητες θέτουν σε εφαρμογή αποτελεσματικό σύστημα υποβολής εκθέσεων συμμόρφωσης, το οποίο είναι κατάλληλο για τις οικείες δομές, τα οικεία περιβάλλοντα λειτουργίας και τα οικεία τοπία απειλών. Το σύστημα υποβολής εκθέσεων συμμόρφωσης είναι ικανό να παρέχει στα διοικητικά όργανα τεκμηριωμένη εικόνα της τρέχουσας κατάστασης όσον αφορά τη διαχείριση των κινδύνων από τις σχετικές οντότητες.

2.2.3. Οι σχετικές οντότητες διενεργούν την παρακολούθηση της συμμόρφωσης σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

2.3. *Ανεξάρτητη αξιολόγηση της ασφάλειας δικτύου και πληροφοριών*

2.3.1. Οι σχετικές οντότητες αξιολογούν ανεξάρτητα την οικεία προσέγγιση όσον αφορά τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών και την εφαρμογή της, συμπεριλαμβανομένων των προσώπων, των διαδικασιών και των τεχνολογιών.

2.3.2. Οι σχετικές οντότητες αναπτύσσουν και διατηρούν διαδικασίες για τη διενέργεια ανεξάρτητων αξιολογήσεων, οι οποίες διενεργούνται από άτομα με κατάλληλη επάρκεια στον τομέα του ελέγχου. Όταν η ανεξάρτητη αξιολόγηση διενεργείται από μέλη του προσωπικού της σχετικής οντότητας, τα πρόσωπα που διενεργούν τις αξιολογήσεις δεν περιλαμβάνονται στη διοικητική ιεραρχία του προσωπικού του υπό αξιολόγηση τομέα. Εάν το μέγεθος των σχετικών οντοτήτων δεν επιτρέπει τον εν λόγω διαχωρισμό της διοικητικής ιεραρχίας, οι σχετικές οντότητες θεσπίζουν εναλλακτικά μέτρα για τη διασφάλιση της αμεροληψίας των αξιολογήσεων.

2.3.3. Τα αποτελέσματα των ανεξάρτητων αξιολογήσεων, συμπεριλαμβανομένων των αποτελεσμάτων της παρακολούθησης της συμμόρφωσης σύμφωνα με το σημείο 2.2. και της παρακολούθησης και μέτρησης σύμφωνα με το σημείο 7, υποβάλλονται στα διοικητικά όργανα. Λαμβάνονται διορθωτικά μέτρα ή γίνεται δεκτός ο υπολειπόμενος κίνδυνος σύμφωνα με τα κριτήρια αποδοχής κινδύνου των σχετικών οντοτήτων.

2.3.4. Οι ανεξάρτητες αξιολογήσεις διενεργούνται σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

3. **Χειρισμός περιστατικών [άρθρο 21 παράγραφος 2 στοιχείο β) της οδηγίας (ΕΕ) 2022/2555]**

3.1. *Πολιτική για τον χειρισμό περιστατικών*

3.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο β) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν και εφαρμόζουν πολιτική για τον χειρισμό περιστατικών στην οποία καθορίζονται οι ρόλοι, οι αρμοδιότητες και οι διαδικασίες για τον εντοπισμό, την ανάλυση, τον περιορισμό ή την αντιμετώπιση περιστατικών, καθώς και για την αποκατάσταση από περιστατικά, την τεκμηρίωση και αναφορά περιστατικών εγκαίρως.

3.1.2. Η πολιτική που αναφέρεται στο σημείο 3.1.1 συνάδει με το σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης έπειτα από καταστροφή που αναφέρεται στο σημείο 4.1. Η πολιτική περιλαμβάνει τα εξής:

α) σύστημα κατηγοριοποίησης περιστατικών που συνάδει με την αξιολόγηση και ταξινόμηση συμβάντων που διενεργείται σύμφωνα με το σημείο 3.4.1.·

β) αποτελεσματικά σχέδια επικοινωνίας, μεταξύ άλλων για την κλιμάκωση και την αναφορά·

γ) ανάθεση ρόλων σε αρμόδιους υπαλλήλους για τον εντοπισμό και την κατάλληλη αντιμετώπιση περιστατικών·

δ) έγγραφα που πρέπει να χρησιμοποιούνται κατά τον εντοπισμό και την αντιμετώπιση περιστατικών, όπως εγχειρίδια αντιμετώπισης περιστατικών, διαγράμματα κλιμάκωσης, κατάλογοι επαφών και υποδείγματα.

3.1.3. Οι ρόλοι, οι αρμοδιότητες και οι διαδικασίες που καθορίζονται στην πολιτική ελέγχονται και αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα και έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους.

3.2. *Παρακολούθηση και καταγραφή*

3.2.1. Οι σχετικές οντότητες καθορίζουν διαδικασίες και χρησιμοποιούν εργαλεία για την παρακολούθηση και την καταγραφή των δραστηριοτήτων στα οικεία συστήματα δικτύου και πληροφοριών για τον εντοπισμό συμβάντων που θα μπορούσαν να θεωρηθούν περιστατικά και την ανάλογη αντίδραση για την άμβλυνση των επιπτώσεων.

3.2.2. Στον βαθμό που αυτό είναι εφικτό, η παρακολούθηση είναι αυτοματοποιημένη και διενεργείται είτε συνεχώς είτε σε τακτά χρονικά διαστήματα, με την επιφύλαξη των επιχειρηματικών δυνατοτήτων. Οι σχετικές οντότητες υλοποιούν τις οικείες δραστηριότητες παρακολούθησης κατά τρόπο που ελαχιστοποιεί τα ψευδώς θετικά αποτελέσματα και τα ψευδώς αρνητικά αποτελέσματα.

3.2.3. Με βάση τις διαδικασίες που αναφέρονται στο σημείο 3.2.1., οι σχετικές οντότητες διατηρούν, τεκμηριώνουν και επανεξετάζουν τα αρχεία καταγραφής. Οι σχετικές οντότητες καταρτίζουν κατάλογο των πάγιων στοιχείων που πρέπει να αποτελέσουν αντικείμενο καταγραφής με βάση τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. Κατά περίπτωση, τα αρχεία καταγραφής περιλαμβάνουν τα εξής:

α) τη σχετική εξερχόμενη και εισερχόμενη κίνηση δικτύων·

β) τη δημιουργία, την τροποποίηση ή τη διαγραφή χρηστών των συστημάτων δικτύου και πληροφοριών των σχετικών οντοτήτων και την επέκταση των αδειών·

γ) την πρόσβαση σε συστήματα και εφαρμογές·

δ) συμβάντα που σχετίζονται με την επαλήθευση ταυτότητας·

ε) κάθε προνομιακή πρόσβαση σε συστήματα και εφαρμογές, καθώς και σε δραστηριότητες που εκτελούνται από διοικητικούς λογαριασμούς·

στ) την πρόσβαση ή τις αλλαγές σε κρίσιμα αρχεία παραμετροποίησης και αντίγραφα ασφαλείας·

ζ) τα αρχεία καταγραφής συμβάντων και τα αρχεία καταγραφής από εργαλεία ασφαλείας, όπως αντιικά λογισμικά, συστήματα ανίχνευσης εισβολών ή τείχη προστασίας·

η) τη χρήση των πόρων του συστήματος, καθώς και τις επιδόσεις τους·

θ) τη φυσική πρόσβαση σε εγκαταστάσεις·

ι) την πρόσβαση σε εξοπλισμό και συσκευές δικτύου και τη χρήση αυτών·

ια) την ενεργοποίηση, τη διακοπή και την παύση των διαφόρων αρχείων καταγραφής·

ιβ) περιβαλλοντικά συμβάντα.

3.2.4. Τα αρχεία καταγραφής επανεξετάζονται τακτικά για τυχόν ασυνήθεις ή ανεπιθύμητες τάσεις. Κατά περίπτωση, οι σχετικές οντότητες καθορίζουν κατάλληλες τιμές για τα όρια συναγερμού. Σε περίπτωση υπέρβασης των καθορισμένων τιμών για το όριο συναγερμού, ενεργοποιείται συναγερμός, κατά περίπτωση, αυτόματα. Οι σχετικές οντότητες εξασφαλίζουν ότι, σε περίπτωση συναγερμού, ενεργοποιείται εγκαίρως ειδική και κατάλληλη απόκριση.

3.2.5. Οι σχετικές οντότητες διατηρούν αρχεία καταγραφής για προκαθορισμένο χρονικό διάστημα και δημιουργούν αντίγραφα ασφαλείας για αυτά, καθώς και τα προστατεύουν από μη εξουσιοδοτημένη πρόσβαση ή αλλαγές.

3.2.6. Στον βαθμό που αυτό είναι εφικτό, οι σχετικές οντότητες διασφαλίζουν ότι όλα τα συστήματα διαθέτουν συγχρονισμένες χρονικές πηγές ώστε να είναι σε θέση να συσχετίζουν αρχεία καταγραφής μεταξύ συστημάτων για την αξιολόγηση συμβάντων. Οι σχετικές οντότητες καταρτίζουν και τηρούν κατάλογο όλων των πάγιων στοιχείων που καταγράφονται και διασφαλίζουν ότι τα συστήματα παρακολούθησης και καταγραφής λειτουργούν εφεδρικά. Η διαθεσιμότητα των συστημάτων παρακολούθησης και καταγραφής παρακολουθείται ανεξάρτητα από τα συστήματα που αυτά παρακολουθούν.

3.2.7. Οι διαδικασίες καθώς και ο κατάλογος των πάγιων στοιχείων που καταγράφονται αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε τακτά χρονικά διαστήματα και μετά από σημαντικά περιστατικά.

3.3. *Αναφορά συμβάντων*

3.3.1. Οι σχετικές οντότητες θέτουν σε εφαρμογή έναν απλό μηχανισμό που επιτρέπει στους υπαλλήλους, στους προμηθευτές και στους πελάτες τους να αναφέρουν ύποπτα συμβάντα.

3.3.2. Οι σχετικές οντότητες κοινοποιούν, κατά περίπτωση, τον μηχανισμό αναφοράς συμβάντων στους προμηθευτές και στους πελάτες τους και εκπαιδεύουν τακτικά τους υπαλλήλους τους σχετικά με τον τρόπο χρήσης του μηχανισμού.

3.4. *Αξιολόγηση και ταξινόμηση συμβάντων*

3.4.1. Οι σχετικές οντότητες αξιολογούν ύποπτα συμβάντα για να προσδιορίσουν κατά πόσον συνιστούν περιστατικά και, εφόσον κάτι τέτοιο διαπιστωθεί, προσδιορίζουν τη φύση και τη σοβαρότητά τους.

3.4.2. Για τους σκοπούς του σημείου 3.4.1., οι σχετικές οντότητες ενεργούν με τον ακόλουθο τρόπο:

α) διενεργούν την αξιολόγηση βάσει προκαθορισμένων κριτηρίων και διαλογής για την ιεράρχηση προτεραιοτήτων όσον αφορά τον περιορισμό και την εξάλειψη των περιστατικών·

β) αξιολογούν την ύπαρξη επαναλαμβανόμενων περιστατικών, όπως αναφέρεται στο άρθρο 4 του παρόντος κανονισμού, σε τριμηνιαία βάση·

γ) αξιολογούν τα κατάλληλα αρχεία καταγραφής για τους σκοπούς της αξιολόγησης και της ταξινόμησης συμβάντων·

δ) θέτουν σε εφαρμογή διαδικασία συσχέτισης και ανάλυσης των αρχείων καταγραφής, και

ε) αξιολογούν και ταξινομούν εκ νέου συμβάντα σε περίπτωση που καταστούν διαθέσιμες νέες πληροφορίες ή μετά από ανάλυση των προηγουμένως διαθέσιμων πληροφοριών.

3.5. *Αντιμετώπιση περιστατικών*

3.5.1. Οι σχετικές οντότητες αντιμετωπίζουν εγκαίρως περιστατικά σύμφωνα με τεκμηριωμένες διαδικασίες.

3.5.2. Οι διαδικασίες αντιμετώπισης περιστατικών περιλαμβάνουν τα ακόλουθα στάδια:

α) περιορισμός του περιστατικού, ώστε να προληφθεί η εξάπλωση των συνεπειών του·

β) εξάλειψη, ώστε να αποφευχθεί η συνέχιση ή η επανεμφάνιση του περιστατικού,

γ) αποκατάσταση μετά από το περιστατικό, όπου απαιτείται.

3.5.3. Οι σχετικές οντότητες καταρτίζουν σχέδια και διαδικασίες επικοινωνίας:

α) με τις ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT) ή, όπου αρμόζει, τις αρμόδιες αρχές, σχετικά με την κοινοποίηση περιστατικών·

β) για την επικοινωνία μεταξύ των μελών του προσωπικού της σχετικής οντότητας και για την επικοινωνία με τα σχετικά ενδιαφερόμενα μέρη εκτός της σχετικής οντότητας.

3.5.4. Οι σχετικές οντότητες καταγράφουν τις δραστηριότητες αντιμετώπισης περιστατικών σύμφωνα με τις διαδικασίες που αναφέρονται στο σημείο 3.2.1. και καταγράφουν αποδεικτικά στοιχεία.

3.5.5. Οι σχετικές οντότητες ελέγχουν σε προγραμματισμένα χρονικά διαστήματα τις οικείες διαδικασίες αντιμετώπισης περιστατικών.

3.6. *Αξιολογήσεις μετά από περιστατικά*

3.6.1. Κατά περίπτωση, οι σχετικές οντότητες διενεργούν αξιολογήσεις μετά από περιστατικά κατόπιν της αποκατάστασης μετά από περιστατικά. Οι αξιολογήσεις μετά από περιστατικά προσδιορίζουν, όπου είναι δυνατόν, τη βαθύτερη αιτία του περιστατικού και οδηγούν σε τεκμηριωμένα διδάγματα που αντλήθηκαν για τη μείωση της εμφάνισης μελλοντικών περιστατικών και των συνεπειών τους.

3.6.2. Οι σχετικές οντότητες διασφαλίζουν ότι οι αξιολογήσεις μετά από περιστατικά συμβάλλουν στη βελτίωση της προσέγγισής τους όσον αφορά την ασφάλεια δικτύου και πληροφοριών, τα μέτρα αντιμετώπισης κινδύνων και τις διαδικασίες χειρισμού, εντοπισμού και αντιμετώπισης περιστατικών.

3.6.3. Οι σχετικές οντότητες επανεξετάζουν σε προγραμματισμένα χρονικά διαστήματα εάν τα περιστατικά οδήγησαν σε αξιολογήσεις μετά από περιστατικά.

4. **Επιχειρησιακή συνέχεια και διαχείριση κρίσεων [άρθρο 21 παράγραφος 2 στοιχείο γ) της οδηγίας (ΕΕ) 2022/2555]**

4.1. *Σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης έπειτα από καταστροφή*

4.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο γ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες καταρτίζουν και διατηρούν σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης έπειτα από καταστροφή, το οποίο εφαρμόζεται σε περίπτωση περιστατικών.

4.1.2. Οι δραστηριότητες των σχετικών οντοτήτων αποκαθίστανται σύμφωνα με το σχέδιο επιχειρησιακής συνέχειας και αποκατάστασης έπειτα από καταστροφή. Το σχέδιο βασίζεται στα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. και περιλαμβάνει, κατά περίπτωση, τα ακόλουθα:

α) σκοπός, πεδίο εφαρμογής και αποδέκτες·

β) ρόλοι και αρμοδιότητες·

γ) σημαντικότερες επαφές και (εσωτερικοί και εξωτερικοί) δίαυλοι επικοινωνίας·

δ) προϋποθέσεις για την ενεργοποίηση και απενεργοποίηση του σχεδίου·

ε) εντολή αποκατάστασης λειτουργιών·

στ) σχέδια αποκατάστασης συγκεκριμένων λειτουργιών, συμπεριλαμβανομένων των στόχων αποκατάστασης·

ζ) απαιτούμενοι πόροι, συμπεριλαμβανομένων των αντιγράφων ασφαλείας και των εφεδρειών·

η) αποκατάσταση και επανέναρξη των δραστηριοτήτων μέσω προσωρινών μέτρων.

4.1.3. Οι σχετικές οντότητες διενεργούν ανάλυση επιχειρηματικών επιπτώσεων για να αξιολογήσουν τον δυνητικό αντίκτυπο σοβαρών διαταράξεων στις οικείες επιχειρηματικές δραστηριότητες και, με βάση τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων, καθορίζουν απαιτήσεις συνέχειας για τα συστήματα δικτύου και πληροφοριών.

4.1.4. Το σχέδιο επιχειρησιακής συνέχειας και το σχέδιο αποκατάστασης έπειτα από καταστροφή ελέγχονται, αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα και έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους. Οι σχετικές οντότητες διασφαλίζουν ότι τα σχέδια ενσωματώνουν τα διδάγματα που αντλήθηκαν από τους εν λόγω ελέγχους.

4.2. *Διαχείριση αντιγράφων ασφαλείας και εφεδρειών*

4.2.1. Οι σχετικές οντότητες διατηρούν αντίγραφα ασφαλείας των δεδομένων και παρέχουν επαρκείς διαθέσιμους πόρους, συμπεριλαμβανομένων των εγκαταστάσεων, των συστημάτων δικτύου και πληροφοριών και του προσωπικού, ώστε να διασφαλίζεται κατάλληλο επίπεδο εφεδρείας.

4.2.2. Με βάση τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. και το σχέδιο επιχειρησιακής συνέχειας, οι σχετικές οντότητες καταρτίζουν εφεδρικά σχέδια τα οποία περιλαμβάνουν τα ακόλουθα:

α) χρόνος αποκατάστασης·

β) διασφάλιση ότι τα αντίγραφα ασφαλείας είναι πλήρη και ακριβή, συμπεριλαμβανομένων των δεδομένων παραμετροποίησης και των δεδομένων που αποθηκεύονται σε περιβάλλον υπηρεσιών υπολογιστικού νέφους·

γ) αποθήκευση αντιγράφων ασφαλείας (είτε επιγραμμικά είτε εκτός διαδικτύου) σε ασφαλείς τοποθεσίες, που δεν βρίσκονται στο ίδιο δίκτυο με το σύστημα και βρίσκονται σε επαρκή απόσταση για την αποφυγή οποιασδήποτε ζημίας από καταστροφή στην κύρια εγκατάσταση·

δ) κατάλληλοι έλεγχοι φυσικής και λογικής πρόσβασης σε αντίγραφα ασφαλείας, σύμφωνα με το επίπεδο ταξινόμησης πάγιων στοιχείων·

ε) αποκατάσταση δεδομένων από αντίγραφα ασφαλείας·

στ) περίοδοι διατήρησης βάσει επιχειρηματικών και κανονιστικών απαιτήσεων.

4.2.3. Οι σχετικές οντότητες διενεργούν τακτικούς ελέγχους ακεραιότητας στα αντίγραφα ασφαλείας.

4.2.4. Με βάση τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. και το σχέδιο επιχειρησιακής συνέχειας, οι σχετικές οντότητες διασφαλίζουν επαρκή διαθεσιμότητα πόρων με τουλάχιστον μερική εφεδρεία των ακόλουθων:

α) συστήματα δικτύου και πληροφοριών·

β) πάγια στοιχεία, συμπεριλαμβανομένων των εγκαταστάσεων, του εξοπλισμού και των προμηθειών·

γ) προσωπικό με την αναγκαία ευθύνη, εξουσία και επάρκεια·

δ) κατάλληλοι δίαυλοι επικοινωνίας.

4.2.5. Κατά περίπτωση, οι σχετικές οντότητες διασφαλίζουν ότι η παρακολούθηση και η προσαρμογή των πόρων, συμπεριλαμβανομένων των εγκαταστάσεων, των συστημάτων και του προσωπικού, βασίζονται δεόντως στις απαιτήσεις αντιγράφων ασφαλείας και εφεδρείας.

4.2.6. Οι σχετικές οντότητες διενεργούν τακτικούς ελέγχους όσον αφορά την αποκατάσταση των αντιγράφων ασφαλείας και την εφεδρεία για να διασφαλίσουν ότι, υπό συνθήκες αποκατάστασης, μπορούν να βασίζονται σε αυτά και ότι καλύπτουν τα αντίγραφα, τις διαδικασίες και τις γνώσεις για την αποτελεσματική αποκατάσταση. Οι σχετικές οντότητες τεκμηριώνουν τα αποτελέσματα των ελέγχων και, όπου απαιτείται, λαμβάνουν διορθωτικά μέτρα.

4.3. *Διαχείριση κρίσεων*

4.3.1. Οι σχετικές οντότητες εφαρμόζουν διαδικασία διαχείρισης κρίσεων.

4.3.2. Οι σχετικές οντότητες διασφαλίζουν ότι η διαδικασία διαχείρισης κρίσεων καλύπτει τουλάχιστον τα ακόλουθα στοιχεία:

α) τους ρόλους και τις αρμοδιότητες του προσωπικού και, κατά περίπτωση, των προμηθευτών και των παρόχων υπηρεσιών, προσδιορίζοντας την κατανομή των ρόλων σε καταστάσεις κρίσης, συμπεριλαμβανομένων των ειδικών μέτρων που πρέπει να ακολουθούνται·

β) τα κατάλληλα μέσα επικοινωνίας μεταξύ των σχετικών οντοτήτων και των σχετικών αρμόδιων αρχών·

γ) την εφαρμογή κατάλληλων μέτρων για τη διασφάλιση της συντήρησης της ασφάλειας των συστημάτων δικτύου και πληροφοριών σε καταστάσεις κρίσης.

Για τους σκοπούς του στοιχείου β), η ροή πληροφοριών μεταξύ των σχετικών οντοτήτων και των σχετικών αρμόδιων αρχών περιλαμβάνει τόσο υποχρεωτικές κοινοποιήσεις, όπως αναφορές περιστατικών και σχετικά χρονοδιαγράμματα, όσο και μη υποχρεωτικές κοινοποιήσεις.

4.3.3. Οι σχετικές οντότητες εφαρμόζουν διαδικασία για τη διαχείριση και τη χρήση των πληροφοριών που λαμβάνουν από τις CSIRT ή, όπου αρμόζει, από τις αρμόδιες αρχές σχετικά με περιστατικά, ευπάθειες, απειλές ή πιθανά μέτρα άμβλυνσης.

4.3.4. Οι σχετικές οντότητες ελέγχουν, αξιολογούν και, κατά περίπτωση, επικαιροποιούν το σχέδιο διαχείρισης κρίσεων σε τακτική βάση ή έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους.

5. **Ασφάλεια της αλυσίδας εφοδιασμού [άρθρο 21 παράγραφος 2 στοιχείο δ) της οδηγίας (ΕΕ) 2022/2555]**

5.1. *Πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού*

5.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο δ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού η οποία διέπει τις σχέσεις με τους οικείους άμεσους προμηθευτές και παρόχους υπηρεσιών, προκειμένου να αμβλυνθούν οι προσδιορισθέντες κίνδυνοι για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Στην πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού, οι σχετικές οντότητες προσδιορίζουν τον ρόλο τους στο πλαίσιο της αλυσίδας εφοδιασμού και τον κοινοποιούν στους οικείους άμεσους προμηθευτές και παρόχους υπηρεσιών.

5.1.2. Στο πλαίσιο της πολιτικής για την ασφάλεια της αλυσίδας εφοδιασμού που αναφέρεται στο σημείο 5.1.1., οι σχετικές οντότητες καθορίζουν κριτήρια για την επιλογή και τη σύναψη συμβάσεων με προμηθευτές και παρόχους υπηρεσιών. Τα εν λόγω κριτήρια περιλαμβάνουν τα εξής:

α) τις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών, συμπεριλαμβανομένων των οικείων διαδικασιών ασφαλούς ανάπτυξης·

β) την ικανότητα των προμηθευτών και των παρόχων υπηρεσιών να πληρούν τις προδιαγραφές κυβερνοασφάλειας που καθορίζονται από τις σχετικές οντότητες·

γ) τη συνολική ποιότητα και ανθεκτικότητα των προϊόντων ΤΠΕ και των υπηρεσιών ΤΠΕ και τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που ενσωματώνονται σε αυτά, συμπεριλαμβανομένων των κινδύνων και του επιπέδου ταξινόμησης των προϊόντων ΤΠΕ και των υπηρεσιών ΤΠΕ·

δ) την ικανότητα των σχετικών οντοτήτων να διαφοροποιούν τις πηγές εφοδιασμού και να περιορίζουν τον εγκλωβισμό σε συγκεκριμένο πάροχο, όπου αρμόζει.

5.1.3. Κατά τη θέσπιση της οικείας πολιτικής για την ασφάλεια της αλυσίδας εφοδιασμού, οι σχετικές οντότητες λαμβάνουν υπόψη τα αποτελέσματα των συντονισμένων εκτιμήσεων κινδύνου για την ασφάλεια κρίσιμων αλυσίδων εφοδιασμού, οι οποίες διενεργούνται σύμφωνα με το άρθρο 22 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, όπου αρμόζει.

5.1.4. Με βάση την πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού και λαμβάνοντας υπόψη τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. του παρόντος παραρτήματος, οι σχετικές οντότητες διασφαλίζουν ότι οι οικείες συμβάσεις με τους προμηθευτές και τους παρόχους υπηρεσιών προσδιορίζουν, κατά περίπτωση μέσω συμφωνιών επιπέδου υπηρεσιών, τα ακόλουθα, κατά περίπτωση:

α) τις απαιτήσεις κυβερνοασφάλειας για τους προμηθευτές ή τους παρόχους υπηρεσιών, συμπεριλαμβανομένων των απαιτήσεων όσον αφορά την ασφάλεια κατά την απόκτηση υπηρεσιών ΤΠΕ ή προϊόντων ΤΠΕ που ορίζονται στο σημείο 6.1.·

β) τις απαιτήσεις σχετικά με την ευαισθητοποίηση, τις δεξιότητες και την κατάρτιση, και κατά περίπτωση τις πιστοποιήσεις, που απαιτούνται από τους υπαλλήλους των προμηθευτών ή των παρόχων υπηρεσιών·

γ) τις απαιτήσεις σχετικά με την επαλήθευση του ιστορικού των υπαλλήλων των προμηθευτών και των παρόχων υπηρεσιών·

δ) την υποχρέωση των προμηθευτών και των παρόχων υπηρεσιών να κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις σχετικές οντότητες περιστατικά που ενέχουν κίνδυνο για την ασφάλεια των συστημάτων δικτύου και πληροφοριών των εν λόγω οντοτήτων·

ε) το δικαίωμα ελέγχου ή το δικαίωμα λήψης εκθέσεων ελέγχου·

στ) την υποχρέωση των προμηθευτών και των παρόχων υπηρεσιών να χειρίζονται ευπάθειες που ενέχουν κίνδυνο για την ασφάλεια των συστημάτων δικτύου και πληροφοριών των σχετικών οντοτήτων·

ζ) τις απαιτήσεις σχετικά με την υπεργολαβία και, σε περίπτωση που οι σχετικές οντότητες επιτρέπουν την υπεργολαβία, τις απαιτήσεις κυβερνοασφάλειας για υπεργολάβους σύμφωνα με τις απαιτήσεις κυβερνοασφάλειας που αναφέρονται στο στοιχείο α)·

η) τις υποχρεώσεις των προμηθευτών και των παρόχων υπηρεσιών κατά τη λήξη της σύμβασης, όπως η ανάκτηση και διάθεση των πληροφοριών που λαμβάνουν οι προμηθευτές και οι πάροχοι υπηρεσιών κατά την άσκηση των καθηκόντων τους.

5.1.5. Οι σχετικές οντότητες λαμβάνουν υπόψη τα στοιχεία που αναφέρονται στα σημεία 5.1.2. και 5.1.3. στο πλαίσιο της διαδικασίας επιλογής νέων προμηθευτών και παρόχων υπηρεσιών, καθώς και στο πλαίσιο της διαδικασίας σύναψης συμβάσεων που αναφέρεται στο σημείο 6.1.

5.1.6. Οι σχετικές οντότητες επανεξετάζουν την πολιτική για την ασφάλεια της αλυσίδας εφοδιασμού και παρακολουθούν, αξιολογούν και, όπου απαιτείται, αναλαμβάνουν δράση σε σχέση με αλλαγές στις πρακτικές κυβερνοασφάλειας των προμηθευτών και των παρόχων υπηρεσιών, σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους ή σημαντικών περιστατικών που σχετίζονται με την παροχή υπηρεσιών ΤΠΕ ή έχουν αντίκτυπο στην ασφάλεια των προϊόντων ΤΠΕ από προμηθευτές και παρόχους υπηρεσιών.

5.1.7. Για τους σκοπούς του σημείου 5.1.6., οι σχετικές οντότητες:

α) παρακολουθούν τακτικά τις εκθέσεις σχετικά με την εφαρμογή των συμφωνιών επιπέδου υπηρεσιών, όπου αρμόζει·

β) εξετάζουν περιστατικά που σχετίζονται με προϊόντα ΤΠΕ και υπηρεσίες ΤΠΕ από προμηθευτές και παρόχους υπηρεσιών·

γ) αξιολογούν την ανάγκη για μη προγραμματισμένες αξιολογήσεις και τεκμηριώνουν τα ευρήματα με κατανοητό τρόπο·

δ) αναλύουν τους κινδύνους που ενέχουν οι αλλαγές που σχετίζονται με προϊόντα ΤΠΕ και υπηρεσίες ΤΠΕ από προμηθευτές και παρόχους υπηρεσιών και, κατά περίπτωση, λαμβάνουν εγκαίρως μέτρα άμβλυνσης.

5.2. *Κατάλογος προμηθευτών και παρόχων υπηρεσιών*

Οι σχετικές οντότητες τηρούν και επικαιροποιούν μητρώο των οικείων άμεσων προμηθευτών και παρόχων υπηρεσιών, το οποίο περιλαμβάνει:

α) σημεία επαφής για κάθε άμεσο προμηθευτή και πάροχο υπηρεσιών·

β) κατάλογο προϊόντων ΤΠΕ, υπηρεσιών ΤΠΕ και διαδικασιών ΤΠΕ που παρέχονται από τον άμεσο προμηθευτή ή πάροχο υπηρεσιών στις σχετικές οντότητες.

6. **Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών [άρθρο 21 παράγραφος 2 στοιχείο ε) της οδηγίας (ΕΕ) 2022/2555]**

6.1. *Ασφάλεια στην απόκτηση υπηρεσιών ΤΠΕ ή προϊόντων ΤΠΕ*

6.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο ε) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες καθορίζουν και εφαρμόζουν διαδικασίες για τη διαχείριση των κινδύνων που απορρέουν από την απόκτηση υπηρεσιών ΤΠΕ ή προϊόντων ΤΠΕ για στοιχεία που είναι ζωτικής σημασίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών των σχετικών οντοτήτων, με βάση την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1., από προμηθευτές ή παρόχους υπηρεσιών καθ' όλη τη διάρκεια του κύκλου ζωής τους.

6.1.2. Για τους σκοπούς του σημείου 6.1.1., οι διαδικασίες που αναφέρονται στο σημείο 6.1.1. περιλαμβάνουν τα εξής:

α) τις απαιτήσεις ασφάλειας που ισχύουν για τις υπηρεσίες ΤΠΕ ή τα προϊόντα ΤΠΕ που πρόκειται να αποκτηθούν·

β) τις απαιτήσεις σχετικά με τις ενημερώσεις ασφαλείας καθ' όλη τη διάρκεια ζωής των υπηρεσιών ΤΠΕ ή των προϊόντων ΤΠΕ ή την αντικατάσταση μετά το τέλος της περιόδου υποστήριξης·

γ) τις πληροφορίες που περιγράφουν τα στοιχεία υλισμικού και λογισμικού που χρησιμοποιούνται στις υπηρεσίες ΤΠΕ ή στα προϊόντα ΤΠΕ·

δ) τις πληροφορίες που περιγράφουν τις εφαρμοζόμενες λειτουργίες κυβερνοασφάλειας των υπηρεσιών ΤΠΕ ή των προϊόντων ΤΠΕ και την παραμετροποίηση που απαιτείται για την ασφαλή λειτουργία τους·

ε) τη διασφάλιση ότι οι υπηρεσίες ΤΠΕ ή τα προϊόντα ΤΠΕ συμμορφώνονται με τις απαιτήσεις ασφάλειας σύμφωνα με το στοιχείο α)·

στ) τις μεθόδους για την επικύρωση της συμμόρφωσης των παρεχόμενων υπηρεσιών ΤΠΕ ή προϊόντων ΤΠΕ με τις καθορισμένες απαιτήσεις ασφάλειας, καθώς και τη τεκμηρίωση των αποτελεσμάτων της επικύρωσης.

6.1.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τις διαδικασίες σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών.

6.2. *Κύκλος ζωής της ασφαλούς ανάπτυξης*

6.2.1. Πριν από την ανάπτυξη συστήματος δικτύου και πληροφοριών, συμπεριλαμβανομένου του λογισμικού, οι σχετικές οντότητες θεσπίζουν κανόνες για την ασφαλή ανάπτυξη συστημάτων δικτύου και πληροφοριών και τους εφαρμόζουν κατά την ανάπτυξη συστημάτων δικτύου και πληροφοριών εσωτερικά ή κατά την εξωτερική ανάθεση της ανάπτυξης συστημάτων δικτύου και πληροφοριών. Οι κανόνες καλύπτουν όλα τα στάδια ανάπτυξης, συμπεριλαμβανομένων των προδιαγραφών, του σχεδιασμού, της ανάπτυξης, της υλοποίησης και των δοκιμών.

6.2.2. Για τους σκοπούς του σημείου 6.2.1., οι σχετικές οντότητες:

α) διενεργούν ανάλυση των απαιτήσεων ασφάλειας κατά τα στάδια των προδιαγραφών και του σχεδιασμού κάθε έργου ανάπτυξης ή απόκτησης που αναλαμβάνεται από τις σχετικές οντότητες ή για λογαριασμό των εν λόγω οντοτήτων·

β) εφαρμόζουν αρχές για τη σχεδίαση ασφαλών συστημάτων και ασφαλών αρχών κωδικοποίησης σε κάθε δραστηριότητα ανάπτυξης συστημάτων πληροφοριών, όπως η προώθηση της κυβερνοασφάλειας εκ σχεδιασμού και οι αρχιτεκτονικές μηδενικής εμπιστοσύνης·

γ) καθορίζουν απαιτήσεις ασφάλειας όσον αφορά τα περιβάλλοντα ανάπτυξης·

δ) θεσπίζουν και εφαρμόζουν διαδικασίες δοκιμών ασφαλείας κατά τον κύκλο ζωής της ανάπτυξης·

ε) επιλέγουν, προστατεύουν και διαχειρίζονται κατάλληλα τα δεδομένα των δοκιμών ασφαλείας·

στ) προβαίνουν σε εξυγίανση και ανωνυμοποίηση των δεδομένων δοκιμών σύμφωνα με την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1.

6.2.3. Για την εξωτερική ανάθεση της ανάπτυξης συστημάτων δικτύου και πληροφοριών, οι σχετικές οντότητες εφαρμόζουν επίσης τις πολιτικές και τις διαδικασίες που αναφέρονται στα σημεία 5 και 6.1.

6.2.4. Οι σχετικές οντότητες αξιολογούν και, όπου απαιτείται, επικαιροποιούν τους οικείους κανόνες ασφαλούς ανάπτυξης σε προγραμματισμένα χρονικά διαστήματα.

6.3. *Διαχείριση παραμετροποίησης*

6.3.1. Οι σχετικές οντότητες λαμβάνουν τα κατάλληλα μέτρα για τον καθορισμό, την τεκμηρίωση, την εφαρμογή και την παρακολούθηση των παραμετροποιήσεων, συμπεριλαμβανομένων των παραμετροποιήσεων ασφαλείας υλισμικού, λογισμικού, υπηρεσιών και δικτύων.

6.3.2. Για τους σκοπούς του σημείου 6.3.1., οι σχετικές οντότητες:

α) καθορίζουν και διασφαλίζουν την ασφάλεια στις παραμετροποιήσεις του υλισμικού, του λογισμικού, των υπηρεσιών και των δικτύων τους·

β) καθορίζουν και εφαρμόζουν διαδικασίες και εργαλεία για την επιβολή των καθορισμένων ασφαλών παραμετροποιήσεων για υλισμικό, λογισμικό, υπηρεσίες και δίκτυα, για τα νεοεγκατεστημένα συστήματα, καθώς και για τα συστήματα σε λειτουργία καθ' όλη τη διάρκεια ζωής τους.

6.3.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τις παραμετροποιήσεις σε προγραμματισμένα χρονικά διαστήματα ή σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

6.4. *Διαχείριση αλλαγών, επισκευές και συντήρηση*

6.4.1. Οι σχετικές οντότητες εφαρμόζουν διαδικασίες διαχείρισης αλλαγών για τον έλεγχο αλλαγών στα συστήματα δικτύου και πληροφοριών. Όπου αρμόζει, οι διαδικασίες συνάδουν με τις γενικές πολιτικές των σχετικών οντοτήτων όσον αφορά τη διαχείριση αλλαγών.

6.4.2. Οι διαδικασίες που αναφέρονται στο σημείο 6.4.1. εφαρμόζονται για εκδόσεις, τροποποιήσεις και αλλαγές έκτακτης ανάγκης οποιουδήποτε λογισμικού και υλισμικού σε λειτουργία και αλλαγές στην παραμετροποίηση. Οι διαδικασίες διασφαλίζουν ότι οι εν λόγω αλλαγές τεκμηριώνονται και, με βάση την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1., υποβάλλονται σε έλεγχο και αξιολογούνται με βάση τον δυνητικό αντίκτυπο πριν από την εφαρμογή τους.

6.4.3. Σε περίπτωση που δεν κατέστη δυνατή η τήρηση των τακτικών διαδικασιών διαχείρισης αλλαγών λόγω έκτακτης ανάγκης, οι σχετικές οντότητες τεκμηριώνουν το αποτέλεσμα της αλλαγής, καθώς και την εξήγηση για τους λόγους για τους οποίους δεν κατέστη δυνατή η τήρηση των διαδικασιών.

6.4.4. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τις διαδικασίες σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

6.5. *Δοκιμές ασφαλείας*

6.5.1. Οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική και διαδικασίες για τις δοκιμές ασφαλείας.

6.5.2. Οι σχετικές οντότητες:

α) καθορίζουν, με βάση την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1., την ανάγκη, το εύρος, τη συχνότητα και το είδος των δοκιμών ασφάλειας·

β) διενεργούν δοκιμές ασφάλειας σύμφωνα με τεκμηριωμένη μεθοδολογία δοκιμών, οι οποίες καλύπτουν τα στοιχεία που προσδιορίζονται ως σημαντικά για την ασφαλή λειτουργία στο πλαίσιο ανάλυσης κινδύνου·

γ) τεκμηριώνουν το είδος, το εύρος, τον χρόνο και τα αποτελέσματα των δοκιμών, συμπεριλαμβανομένης της αξιολόγησης της κρισιμότητας και των μέτρων άμβλυνσης για κάθε εύρημα·

δ) εφαρμόζουν μέτρα άμβλυνσης σε περίπτωση κρίσιμων ευρημάτων.

6.5.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τις οικείες πολιτικές για τις δοκιμές ασφάλειας σε προγραμματισμένα χρονικά διαστήματα.

6.6. *Διαχείριση διορθώσεων ασφαλείας*

6.6.1. Οι σχετικές οντότητες προσδιορίζουν και εφαρμόζουν διαδικασίες που συνάδουν με τις διαδικασίες διαχείρισης αλλαγών που αναφέρονται στο σημείο 6.4.1., καθώς και με τη διαχείριση ευπαθειών, τη διαχείριση κινδύνων και άλλες σχετικές διαδικασίες διαχείρισης, ώστε να διασφαλίζεται ότι:

α) οι διορθώσεις ασφαλείας εφαρμόζονται εντός εύλογου χρονικού διαστήματος από τη στιγμή που καθίστανται διαθέσιμες·

β) οι διορθώσεις ασφαλείας υποβάλλονται σε δοκιμές πριν από την εφαρμογή τους σε συστήματα παραγωγής·

γ) οι διορθώσεις ασφαλείας προέρχονται από αξιόπιστες πηγές και ελέγχονται ως προς την ακεραιότητά τους·

δ) εφαρμόζονται πρόσθετα μέτρα και γίνονται αποδεκτοί υπολειπόμενοι κίνδυνοι σε περιπτώσεις όπου δεν υπάρχει διαθέσιμη διόρθωση ή αυτή δεν εφαρμόζεται σύμφωνα με το σημείο 6.6.2.

6.6.2. Κατά παρέκκλιση από το σημείο 6.6.1. στοιχείο α), οι σχετικές οντότητες μπορούν να επιλέξουν να μην εφαρμόσουν διορθώσεις ασφαλείας όταν τα μειονεκτήματα της εφαρμογής των διορθώσεων ασφαλείας υπερτερούν των οφελών για την κυβερνοασφάλεια. Οι σχετικές οντότητες τεκμηριώνουν δεόντως και αποδεικνύουν τους λόγους κάθε τέτοιας απόφασης.

6.7. *Ασφάλεια δικτύου*

6.7.1. Οι σχετικές οντότητες λαμβάνουν τα κατάλληλα μέτρα για την προστασία των οικείων συστημάτων δικτύου και πληροφοριών από κυβερνοαπειλές.

6.7.2. Για τους σκοπούς του σημείου 6.7.1., οι σχετικές οντότητες:

α) τεκμηριώνουν την αρχιτεκτονική του δικτύου με κατανοητό και ενημερωμένο τρόπο·

β) καθορίζουν και εφαρμόζουν ελέγχους για την προστασία των τομέων εσωτερικού δικτύου των σχετικών οντοτήτων από μη εξουσιοδοτημένη πρόσβαση·

γ) σχεδιάζουν τη διενέργεια ελέγχων για την αποτροπή της πρόσβασης σε δίκτυο και της επικοινωνίας μέσω δικτύου, οι οποίες δεν απαιτούνται για τη λειτουργία των σχετικών οντοτήτων·

δ) καθορίζουν και εφαρμόζουν ελέγχους για την εξ αποστάσεως πρόσβαση σε συστήματα δικτύου και πληροφοριών, συμπεριλαμβανομένης της πρόσβασης των παρόχων υπηρεσιών·

ε) δεν προβαίνουν σε χρήση των συστημάτων που χρησιμοποιούνται για τη διαχείριση της εφαρμογής της πολιτικής ασφάλειας για άλλους σκοπούς·

στ) απαγορεύουν ρητά ή απενεργοποιούν τις μη αναγκαίες συνδέσεις και υπηρεσίες·

ζ) κατά περίπτωση, επιτρέπουν αποκλειστικά την πρόσβαση στα συστήματα δικτύου και πληροφοριών των σχετικών οντοτήτων από συσκευές εξουσιοδοτημένες από τις εν λόγω οντότητες·

η) επιτρέπουν τις συνδέσεις των παρόχων υπηρεσιών μόνο μετά από αίτηση εξουσιοδότησης και για καθορισμένο χρονικό διάστημα, όπως η διάρκεια της εργασίας συντήρησης·

θ) καθιερώνουν επικοινωνία μεταξύ διακριτών συστημάτων μόνο μέσω αξιόπιστων διαύλων που είναι απομονωμένοι με τη χρήση λογικού, κρυπτογραφικού ή φυσικού διαχωρισμού από άλλους διαύλους επικοινωνίας και παρέχουν ασφαλή προσδιορισμό των οικείων τελικών σημείων και προστασία των δεδομένων του διαύλου από τροποποίηση ή γνωστοποίηση·

ι) εγκρίνουν σχέδιο εφαρμογής για την πλήρη μετάβαση σε πρωτόκολλα επικοινωνίας επιπέδου δικτύου τελευταίας γενιάς με ασφαλή, κατάλληλο και σταδιακό τρόπο και θεσπίζουν μέτρα για την επιτάχυνση της εν λόγω μετάβασης·

ια) εγκρίνουν σχέδιο εφαρμογής για την ανάπτυξη διεθνώς συμφωνημένων και διαλειτουργικών σύγχρονων προτύπων επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου για την ασφάλεια των επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου με σκοπό τον μετριασμό των ευπαθειών που συνδέονται με απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο και τη θέσπιση μέτρων για την επιτάχυνση της εν λόγω ανάπτυξης·

ιβ) εφαρμόζουν βέλτιστες πρακτικές για την ασφάλεια του DNS, καθώς και για την ασφάλεια της δρομολόγησης στο διαδίκτυο και την υγιεινή της δρομολόγησης της κίνησης που προέρχεται από το δίκτυο και προορίζεται για αυτό.

6.7.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τα εν λόγω μέτρα σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

6.8. *Κατάτμηση δικτύου*

6.8.1. Οι σχετικές οντότητες κατατέμνουν τα συστήματα σε δίκτυα ή ζώνες σύμφωνα με τα αποτελέσματα της εκτίμησης κινδύνου που αναφέρεται στο σημείο 2.1. Διαχωρίζουν τα οικεία συστήματα και δίκτυα από συστήματα και δίκτυα τρίτων μερών.

6.8.2. Για τον σκοπό αυτό, οι σχετικές οντότητες:

α) εξετάζουν τη λειτουργική, λογική και φυσική σχέση, συμπεριλαμβανομένης της τοποθεσίας, μεταξύ αξιόπιστων συστημάτων και υπηρεσιών·

β) παρέχουν πρόσβαση σε δίκτυο ή ζώνη βάσει αξιολόγησης των οικείων απαιτήσεων ασφάλειας·

γ) διατηρούν συστήματα ζωτικής σημασίας για τη λειτουργία των σχετικών οντοτήτων ή για την ασφάλεια σε ζώνες ασφαλείας·

δ) αναπτύσσουν αποστρατιωτικοποιημένη ζώνη εντός των οικείων δικτύων επικοινωνίας για τη διασφάλιση ασφαλούς επικοινωνίας που προέρχεται από τα οικεία δίκτυα ή προορίζεται για αυτά·

ε) περιορίζουν την πρόσβαση και τις επικοινωνίες μεταξύ και εντός των ζωνών στις αναγκαίες για τη λειτουργία των σχετικών οντοτήτων ή για την ασφάλεια·

στ) διαχωρίζουν το ειδικό δίκτυο για τη διαχείριση συστημάτων δικτύου και πληροφοριών από το επιχειρησιακό δίκτυο των σχετικών οντοτήτων·

ζ) διαχωρίζουν τους διαύλους διαχείρισης δικτύου από την κίνηση άλλων δικτύων·

η) διαχωρίζουν τα συστήματα παραγωγής για τις υπηρεσίες των σχετικών οντοτήτων από τα συστήματα που χρησιμοποιούνται στην ανάπτυξη και στις δοκιμές, συμπεριλαμβανομένων των αντιγράφων ασφαλείας.

6.8.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την κατάτμηση δικτύου σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

6.9. *Προστασία από κακόβουλο και μη εξουσιοδοτημένο λογισμικό*

6.9.1. Οι σχετικές οντότητες προστατεύουν τα οικεία συστήματα δικτύου και πληροφοριών από κακόβουλο και μη εξουσιοδοτημένο λογισμικό.

6.9.2. Για τον σκοπό αυτό, οι σχετικές οντότητες εφαρμόζουν ιδίως μέτρα για τον εντοπισμό ή την πρόληψη της χρήσης κακόβουλου ή μη εξουσιοδοτημένου λογισμικού. Οι σχετικές οντότητες διασφαλίζουν, κατά περίπτωση, ότι τα οικεία συστήματα δικτύου και πληροφοριών είναι εξοπλισμένα με λογισμικό εντοπισμού και απόκρισης, το οποίο επικαιροποιείται τακτικά σύμφωνα με την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1. και τις συμβατικές συμφωνίες με τους παρόχους.

6.10. *Χειρισμός και γνωστοποίηση ευπαθειών*

6.10.1. Οι σχετικές οντότητες λαμβάνουν πληροφορίες σχετικά με τεχνικές ευπάθειες στα οικεία συστήματα δικτύου και πληροφοριών, αξιολογούν την έκθεσή τους στις εν λόγω ευπάθειες και λαμβάνουν κατάλληλα μέτρα για τη διαχείριση των ευπαθειών.

6.10.2. Για τους σκοπούς του σημείου 6.10.1., οι σχετικές οντότητες:

α) παρακολουθούν τις πληροφορίες σχετικά με τις ευπάθειες μέσω κατάλληλων διαύλων, όπως ανακοινώσεις των CSIRT, αρμόδιες αρχές ή πληροφορίες που παρέχονται από προμηθευτές ή παρόχους υπηρεσιών·

β) διενεργούν, κατά περίπτωση, σαρώσεις ευπαθειών και καταγράφουν αποδεικτικά στοιχεία των αποτελεσμάτων των σαρώσεων, σε προγραμματισμένα χρονικά διαστήματα·

γ) αντιμετωπίζουν, χωρίς αδικαιολόγητη καθυστέρηση, τις ευπάθειες που προσδιορίζονται από τις σχετικές οντότητες ως κρίσιμες για τις οικείες δραστηριότητες·

δ) διασφαλίζουν ότι ο οικείος χειρισμός των ευπαθειών είναι συμβατός με τις οικείες διαδικασίες διαχείρισης αλλαγών, διαχείρισης διορθώσεων ασφαλείας, διαχείρισης κινδύνων και διαχείρισης περιστατικών·

ε) θεσπίζουν διαδικασία για τη γνωστοποίηση ευπαθειών σύμφωνα με την ισχύουσα εθνική πολιτική για τη συντονισμένη γνωστοποίηση ευπαθειών.

6.10.3. Όταν δικαιολογείται από τον δυνητικό αντίκτυπο της ευπάθειας, οι σχετικές οντότητες καταρτίζουν και εφαρμόζουν σχέδιο για την άμβλυνση της ευπάθειας. Σε άλλες περιπτώσεις, οι σχετικές οντότητες τεκμηριώνουν και αποδεικνύουν τον λόγο για τον οποίο η ευπάθεια δεν απαιτεί αποκατάσταση.

6.10.4. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν σε προγραμματισμένα χρονικά διαστήματα τους διαύλους που χρησιμοποιούν για την παρακολούθηση των πληροφοριών σχετικά με ευπάθειες.

7. **Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας [άρθρο 21 παράγραφος 2 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555]**

7.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική και διαδικασίες για την αξιολόγηση του κατά πόσον τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που λαμβάνονται από τη σχετική οντότητα εφαρμόζονται και διατηρούνται αποτελεσματικά.

7.2. Η πολιτική και οι διαδικασίες που αναφέρονται στο σημείο 7.1. λαμβάνουν υπόψη τα αποτελέσματα της εκτίμησης κινδύνου σύμφωνα με το σημείο 2.1. και προηγούμενα σημαντικά περιστατικά. Οι σχετικές οντότητες προσδιορίζουν:

α) τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που πρέπει να παρακολουθούνται και να μετρώνται, συμπεριλαμβανομένων των διαδικασιών και των ελέγχων·

β) τις μεθόδους για την παρακολούθηση, τη μέτρηση, την ανάλυση και την αξιολόγηση, κατά περίπτωση, για τη διασφάλιση έγκυρων αποτελεσμάτων·

γ) τον χρόνο διενέργειας της παρακολούθησης και της μέτρησης·

δ) το πρόσωπο που είναι υπεύθυνο για την παρακολούθηση και τη μέτρηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας·

ε) τον χρόνο ανάλυσης και αξιολόγησης των αποτελεσμάτων της παρακολούθησης και της μέτρησης·

στ) το πρόσωπο που θα πρέπει να αναλύσει και να αξιολογήσει τα αποτελέσματα αυτά.

7.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την πολιτική και τις διαδικασίες σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

8. **Βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια [άρθρο 21 παράγραφος 2 στοιχείο ζ) της οδηγίας (ΕΕ) 2022/2555]**

8.1. *Ευαισθητοποίηση και βασικές πρακτικές κυβερνοϋγιεινής*

8.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο ζ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες διασφαλίζουν ότι οι υπάλληλοί τους, συμπεριλαμβανομένων των μελών των διοικητικών οργάνων, καθώς και οι άμεσοι προμηθευτές και πάροχοι υπηρεσιών γνωρίζουν τους κινδύνους, ενημερώνονται για τη σημασία της κυβερνοασφάλειας και εφαρμόζουν πρακτικές κυβερνοϋγιεινής.

8.1.2. Για τους σκοπούς του σημείου 8.1.1., οι σχετικές οντότητες προσφέρουν στους υπαλλήλους τους, συμπεριλαμβανομένων των μελών των διοικητικών οργάνων, καθώς και στους άμεσους προμηθευτές και παρόχους υπηρεσιών, κατά περίπτωση, σύμφωνα με το σημείο 5.1.4., πρόγραμμα ευαισθητοποίησης, το οποίο:

α) προγραμματίζεται βάσει χρονοδιαγράμματος, ώστε οι δραστηριότητες να επαναλαμβάνονται και να καλύπτουν νέους υπαλλήλους·

β) θεσπίζεται σύμφωνα με την πολιτική για την ασφάλεια δικτύου και πληροφοριών, τις πολιτικές για συγκεκριμένα θέματα και τις σχετικές διαδικασίες για την ασφάλεια δικτύου και πληροφοριών·

γ) καλύπτουν τις σχετικές κυβερνοαπειλές, τα ισχύοντα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, τα σημεία επαφής και τους πόρους για πρόσθετες πληροφορίες και συμβουλές σε θέματα κυβερνοασφάλειας, καθώς και τις πρακτικές κυβερνοϋγιεινής για τους χρήστες.

8.1.3. Το πρόγραμμα ευαισθητοποίησης ελέγχεται, κατά περίπτωση, από άποψη αποτελεσματικότητας. Το πρόγραμμα ευαισθητοποίησης επικαιροποιείται και προσφέρεται σε προγραμματισμένα χρονικά διαστήματα, λαμβανομένων υπόψη των αλλαγών στις πρακτικές κυβερνοϋγιεινής, καθώς και του υφιστάμενου τοπίου απειλών και των κινδύνων για τις σχετικές οντότητες.

8.2. *Κατάρτιση στην κυβερνοασφάλεια*

8.2.1. Οι σχετικές οντότητες προσδιορίζουν τους υπαλλήλους, των οποίων οι ρόλοι απαιτούν σύνολα δεξιοτήτων και εμπειρογνωσία σχετικά με την κυβερνοασφάλεια, και διασφαλίζουν ότι λαμβάνουν τακτική κατάρτιση σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

8.2.2. Οι σχετικές οντότητες καταρτίζουν, υλοποιούν και εφαρμόζουν πρόγραμμα κατάρτισης σύμφωνα με την πολιτική για την ασφάλεια δικτύου και πληροφοριών, πολιτικές για συγκεκριμένα θέματα και άλλες σχετικές διαδικασίες για την ασφάλεια δικτύου και πληροφοριών, το οποίο καθορίζει τις ανάγκες κατάρτισης για ορισμένους ρόλους και θέσεις βάσει κριτηρίων.

8.2.3. Η κατάρτιση που αναφέρεται στο σημείο 8.2.1. είναι συναφής με τη θέση εργασίας του υπαλλήλου και η αποτελεσματικότητά της αξιολογείται. Η κατάρτιση λαμβάνει υπόψη τα ισχύοντα μέτρα ασφάλειας και καλύπτει τα ακόλουθα:

α) οδηγίες σχετικά με την ασφαλή παραμετροποίηση και λειτουργία των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων των φορητών συσκευών·

β) ενημέρωση σχετικά με γνωστές κυβερνοαπειλές·

γ) κατάρτιση όσον αφορά τη συμπεριφορά σε περίπτωση συμβάντων σχετικών με την ασφάλεια.

8.2.4. Οι σχετικές οντότητες εφαρμόζουν κατάρτιση στα μέλη του προσωπικού που αναλαμβάνουν νέες θέσεις ή ρόλους που απαιτούν σύνολα δεξιοτήτων και εμπειρογνωσία που είναι σχετικά με την ασφάλεια.

8.2.5. Το πρόγραμμα επικαιροποιείται και υλοποιείται περιοδικά λαμβάνοντας υπόψη τις ισχύουσες πολιτικές και κανόνες, τους ανατεθέντες ρόλους, τις αρμοδιότητες, καθώς και τις γνωστές κυβερνοαπειλές και τις τεχνολογικές εξελίξεις.

9. **Κρυπτογραφία [άρθρο 21 παράγραφος 2 στοιχείο η) της οδηγίας (ΕΕ) 2022/2555]**

9.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο η) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική και διαδικασίες που σχετίζονται με την κρυπτογραφία, με σκοπό τη διασφάλιση επαρκούς και αποτελεσματικής χρήσης της κρυπτογραφίας για την προστασία της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των δεδομένων σύμφωνα με την ταξινόμηση πάγιων στοιχείων των σχετικών οντοτήτων και τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1.

9.2. Η πολιτική και οι διαδικασίες που αναφέρονται στο σημείο 9.1. καθορίζουν:

α) σύμφωνα με την ταξινόμηση των πάγιων στοιχείων από τις σχετικές οντότητες, το είδος, την αυστηρότητα και την ποιότητα των μέτρων κρυπτογραφίας που απαιτούνται για την προστασία των πάγιων στοιχείων των σχετικών οντοτήτων, συμπεριλαμβανομένων των αδρανών δεδομένων και των δεδομένων υπό διαμετακόμιση·

β) με βάση το στοιχείο α), τα πρωτόκολλα ή τις οικογένειες πρωτοκόλλων που πρόκειται να εγκριθούν, καθώς και τους κρυπτογραφικούς αλγόριθμους, την ισχύ των κρυπτογραφικών κωδικών, τις κρυπτογραφικές λύσεις και τις πρακτικές χρήσης που πρέπει να εγκρίνονται και να απαιτούνται για χρήση στις σχετικές οντότητες, ακολουθώντας, κατά περίπτωση, προσέγγιση κρυπτογραφικής ευελιξίας·

γ) την προσέγγιση των σχετικών οντοτήτων όσον αφορά τη διαχείριση κλειδιών, συμπεριλαμβανομένων, κατά περίπτωση, μεθόδων για τα ακόλουθα:

i) δημιουργία διαφορετικών κλειδιών για συστήματα και εφαρμογές κρυπτογραφίας·

ii) έκδοση και απόκτηση πιστοποιητικών δημόσιων κλειδιών·

iii) διανομή κλειδιών στις σχετικές οντότητες, συμπεριλαμβανομένου του τρόπου ενεργοποίησης των κλειδιών κατά τη λήψη τους·

iv) αποθήκευση κλειδιών, συμπεριλαμβανομένου του τρόπου με τον οποίο οι εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε κλειδιά·

v) αλλαγή ή επικαιροποίηση κλειδιών, συμπεριλαμβανομένων κανόνων σχετικά με τον χρόνο και τον τρόπο αλλαγής κλειδιών·

vi) αντιμετώπιση των υπονομευμένων κλειδιών·

vii) ανάκληση κλειδιών, συμπεριλαμβανομένου του τρόπου ανάκλησης ή απενεργοποίησης κλειδιών·

viii) ανάκτηση απολεσθέντων ή αλλοιωμένων κλειδιών·

ix) υποστήριξη ή αρχειοθέτηση κλειδιών·

x) καταστροφή κλειδιών·

xi) καταγραφή και έλεγχος δραστηριοτήτων που σχετίζονται με τη διαχείριση κλειδιών·

xii) καθορισμός ημερομηνιών ενεργοποίησης και απενεργοποίησης για κλειδιά ώστε να διασφαλίζεται ότι τα κλειδιά μπορούν να χρησιμοποιηθούν μόνο για το καθορισμένο χρονικό διάστημα σύμφωνα με τους κανόνες του οργανισμού για τη διαχείριση των κλειδιών.

9.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την οικεία πολιτική και τις οικείες διαδικασίες σε προγραμματισμένα χρονικά διαστήματα, λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας στον τομέα της κρυπτογραφίας.

10. **Ασφάλεια ανθρώπινων πόρων [άρθρο 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555]**

10.1. *Ασφάλεια ανθρώπινων πόρων*

10.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες διασφαλίζουν ότι οι υπάλληλοί τους και οι οικείοι άμεσοι προμηθευτές και πάροχοι υπηρεσιών, κατά περίπτωση, κατανοούν τις ευθύνες τους στον τομέα της ασφάλειας και αναλαμβάνουν τη δέσμευση που τους αναλογεί, κατά περίπτωση για τις προσφερόμενες υπηρεσίες και τη θέση εργασίας και σύμφωνα με την πολιτική των σχετικών οντοτήτων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.

10.1.2. Η απαίτηση που αναφέρεται στο σημείο 10.1.1. περιλαμβάνει τα ακόλουθα:

α) μηχανισμούς που διασφαλίζουν ότι όλοι οι υπάλληλοι, οι άμεσοι προμηθευτές και πάροχοι υπηρεσιών, κατά περίπτωση, κατανοούν και ακολουθούν τις τυποποιημένες πρακτικές κυβερνοϋγιεινής που εφαρμόζουν οι σχετικές οντότητες σύμφωνα με το σημείο 8.1.·

β) μηχανισμούς που διασφαλίζουν ότι όλοι οι χρήστες με διοικητική ή προνομιακή πρόσβαση γνωρίζουν τους ρόλους, τις αρμοδιότητες και τις εξουσίες τους και ενεργούν σύμφωνα με αυτούς·

γ) μηχανισμούς που διασφαλίζουν ότι τα μέλη των διοικητικών οργάνων κατανοούν και ενεργούν σύμφωνα με τον ρόλο, τις αρμοδιότητες και τις εξουσίες τους όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών·

δ) μηχανισμούς πρόσληψης προσωπικού ειδικευμένου για τους αντίστοιχους ρόλους, όπως έλεγχοι αναφοράς, διαδικασίες ελέγχου, επικύρωση πιστοποιήσεων ή γραπτές δοκιμασίες.

10.1.3. Οι σχετικές οντότητες αξιολογούν την ανάθεση συγκεκριμένων ρόλων στο προσωπικό, όπως αναφέρεται στο σημείο 1.2., καθώς και την εκ μέρους τους δέσμευση ανθρώπινων πόρων για τον σκοπό αυτό, σε προγραμματισμένα χρονικά διαστήματα και τουλάχιστον ετησίως. Επικαιροποιούν την ανάθεση, όπου απαιτείται.

10.2. *Επαλήθευση ιστορικού*

10.2.1. Οι σχετικές οντότητες διασφαλίζουν, στον βαθμό που αυτό είναι εφικτό, την επαλήθευση του ιστορικού των υπαλλήλων τους και, όπου αρμόζει, των οικείων άμεσων προμηθευτών και παρόχων υπηρεσιών σύμφωνα με το σημείο 5.1.4., εφόσον είναι αναγκαίο για τους ρόλους, τις αρμοδιότητες και τις εξουσίες τους.

10.2.2. Για τους σκοπούς του σημείου 10.2.1., οι σχετικές οντότητες:

α) θεσπίζουν κριτήρια, τα οποία καθορίζουν τους ρόλους, τις αρμοδιότητες και τις εξουσίες που ασκούνται μόνο από πρόσωπα των οποίων το ιστορικό έχει επαληθευτεί·

β) διασφαλίζουν ότι η επαλήθευση που αναφέρεται στο σημείο 10.2.1. διενεργείται στα εν λόγω πρόσωπα πριν αρχίσουν να ασκούν αυτούς τους ρόλους, τις αρμοδιότητες και τις εξουσίες, οι οποίοι λαμβάνουν υπόψη τους ισχύοντες νόμους, κανονισμούς και δεοντολογία κατ' αναλογία προς τις επιχειρηματικές απαιτήσεις, την ταξινόμηση πάγιων στοιχείων όπως αναφέρεται στο σημείο 12.1. και τα συστήματα δικτύου και πληροφοριών στα οποία πρέπει να έχουν πρόσβαση, καθώς και τους διαφαινόμενους κινδύνους.

10.2.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την πολιτική σε προγραμματισμένα χρονικά διαστήματα και την επικαιροποιούν όπου απαιτείται.

10.3. *Διαδικασίες λήξης ή αλλαγής της απασχόλησης*

10.3.1. Οι σχετικές οντότητες διασφαλίζουν ότι οι αρμοδιότητες και τα καθήκοντα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών που εξακολουθούν να ισχύουν μετά τη λήξη ή την αλλαγή της απασχόλησης των υπαλλήλων τους καθορίζονται και επιβάλλονται στο πλαίσιο σύμβασης.

10.3.2. Για τους σκοπούς του σημείου 10.3.1., οι σχετικές οντότητες περιλαμβάνουν στους όρους και στις προϋποθέσεις απασχόλησης, σύμβασης ή συμφωνίας του προσώπου τις αρμοδιότητες και τα καθήκοντα που εξακολουθούν να ισχύουν μετά τη λήξη της απασχόλησης ή της σύμβασης, όπως ρήτρες εμπιστευτικότητας.

10.4. *Πειθαρχική διαδικασία*

10.4.1. Οι σχετικές οντότητες θεσπίζουν, κοινοποιούν και διατηρούν πειθαρχική διαδικασία για τον χειρισμό παραβιάσεων των πολιτικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Η διαδικασία λαμβάνει υπόψη τις σχετικές νομικές, καταστατικές, συμβατικές και επιχειρηματικές απαιτήσεις.

10.4.2. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τη πειθαρχική διαδικασία σε προγραμματισμένα χρονικά διαστήματα και όταν είναι αναγκαίο λόγω νομικών αλλαγών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

11. **Έλεγχος πρόσβασης [άρθρο 21 παράγραφος 2 στοιχεία θ) και ι) της οδηγίας (ΕΕ) 2022/2555]**

11.1. *Πολιτική ελέγχου πρόσβασης*

11.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες θεσπίζουν, τεκμηριώνουν και εφαρμόζουν πολιτικές ελέγχου λογικής και φυσικής πρόσβασης για την πρόσβαση στα οικεία συστήματα δικτύου και πληροφοριών, με βάση τις επιχειρηματικές απαιτήσεις, καθώς και τις απαιτήσεις ασφάλειας των συστημάτων δικτύου και πληροφοριών.

11.1.2. Οι πολιτικές που αναφέρονται στο σημείο 11.1.1.:

α) αφορούν την πρόσβαση προσώπων, συμπεριλαμβανομένων του προσωπικού, των επισκεπτών και εξωτερικών οντοτήτων, όπως οι προμηθευτές και οι πάροχοι υπηρεσιών·

β) αφορούν την πρόσβαση των συστημάτων δικτύου και πληροφοριών·

γ) διασφαλίζουν ότι η πρόσβαση παρέχεται μόνο σε χρήστες που έχουν ταυτοποιηθεί επαρκώς.

11.1.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν τις εν λόγω πολιτικές σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

11.2. *Διαχείριση των δικαιωμάτων πρόσβασης*

11.2.1. Οι σχετικές οντότητες παρέχουν, τροποποιούν, αφαιρούν και τεκμηριώνουν δικαιώματα πρόσβασης σε συστήματα δικτύου και πληροφοριών σύμφωνα με την πολιτική ελέγχου πρόσβασης που αναφέρεται στο σημείο 11.1.

11.2.2. Οι σχετικές οντότητες:

α) εκχωρούν και ανακαλούν δικαιώματα πρόσβασης με βάση τις αρχές της ανάγκης γνώσης, των ελάχιστων προνομίων και του διαχωρισμού των καθηκόντων·

β) διασφαλίζουν ότι τα δικαιώματα πρόσβασης τροποποιούνται αναλόγως κατά τη λήξη ή την αλλαγή της απασχόλησης·

γ) διασφαλίζουν ότι η πρόσβαση στα συστήματα δικτύου και πληροφοριών επιτρέπεται από τα αρμόδια πρόσωπα·

δ) διασφαλίζουν ότι τα δικαιώματα πρόσβασης καλύπτουν κατάλληλα την πρόσβαση τρίτων, όπως οι επισκέπτες, οι προμηθευτές και οι πάροχοι υπηρεσιών, ιδίως με τον περιορισμό των δικαιωμάτων πρόσβασης ως προς το πεδίο εφαρμογής και τη διάρκεια·

ε) τηρούν μητρώο των παρεχόμενων δικαιωμάτων πρόσβασης·

στ) εφαρμόζουν την καταγραφή για τη διαχείριση των δικαιωμάτων πρόσβασης.

11.2.3. Οι σχετικές οντότητες αξιολογούν τα δικαιώματα πρόσβασης σε προγραμματισμένα χρονικά διαστήματα και τα τροποποιούν βάσει οργανωτικών αλλαγών. Οι σχετικές οντότητες τεκμηριώνουν τα αποτελέσματα της αξιολόγησης, συμπεριλαμβανομένων των αναγκαίων αλλαγών στα δικαιώματα πρόσβασης.

11.3. *Προνομιακοί λογαριασμοί και λογαριασμοί διαχείρισης συστήματος*

11.3.1. Οι σχετικές οντότητες διατηρούν πολιτικές για τη διαχείριση προνομιακών λογαριασμών και λογαριασμών διαχείρισης συστήματος στο πλαίσιο της πολιτικής ελέγχου πρόσβασης που αναφέρεται στο σημείο 11.1.

11.3.2. Οι πολιτικές που αναφέρονται στο σημείο 11.3.1.:

α) θεσπίζουν αυστηρές διαδικασίες ταυτοποίησης, επαλήθευσης ταυτότητας, όπως η πολυπαραγοντική επαλήθευση ταυτότητας, και διαδικασίες εξουσιοδότησης για προνομιακούς λογαριασμούς και λογαριασμούς διαχείρισης συστημάτων·

β) δημιουργούν ειδικούς λογαριασμούς που χρησιμοποιούνται αποκλειστικά για τις λειτουργίες διαχείρισης του συστήματος, όπως η εγκατάσταση, η παραμετροποίηση, η διαχείριση ή η συντήρηση·

γ) εξατομικεύουν και περιορίζουν τα προνόμια διαχείρισης του συστήματος στον μέγιστο δυνατό βαθμό·

δ) προβλέπουν ότι οι λογαριασμοί διαχείρισης του συστήματος χρησιμοποιούνται μόνο για τη σύνδεση με συστήματα διαχείρισης συστημάτων.

11.3.3. Οι σχετικές οντότητες αξιολογούν τα δικαιώματα πρόσβασης σε προνομιακούς λογαριασμούς και λογαριασμούς διαχείρισης συστήματος σε προγραμματισμένα χρονικά διαστήματα και τα τροποποιούν βάσει οργανωτικών αλλαγών, και τεκμηριώνουν τα αποτελέσματα της αξιολόγησης, συμπεριλαμβανομένων των αναγκαίων αλλαγών στα δικαιώματα πρόσβασης.

11.4. *Συστήματα διαχείρισης*

11.4.1. Οι σχετικές οντότητες περιορίζουν και ελέγχουν τη χρήση των συστημάτων διαχείρισης συστήματος σύμφωνα με την πολιτική ελέγχου πρόσβασης που αναφέρεται στο σημείο 11.1.

11.4.2. Για τον σκοπό αυτό, οι σχετικές οντότητες:

α) χρησιμοποιούν συστήματα διαχείρισης συστήματος μόνο για σκοπούς διαχείρισης του συστήματος και όχι για άλλες λειτουργίες·

β) διαχωρίζουν λογικά τα εν λόγω συστήματα από το λογισμικό εφαρμογών που δεν χρησιμοποιείται για σκοπούς διαχείρισης συστήματος·

γ) προστατεύουν την πρόσβαση στα συστήματα διαχείρισης συστήματος μέσω επαλήθευσης ταυτότητας και κρυπτογράφησης.

11.5. *Ταυτοποίηση*

11.5.1. Οι σχετικές οντότητες διαχειρίζονται τον πλήρη κύκλο ζωής των ταυτοτήτων των συστημάτων δικτύου και πληροφοριών και των χρηστών τους.

11.5.2. Για τον σκοπό αυτό, οι σχετικές οντότητες:

α) δημιουργούν μοναδικές ταυτότητες για τα συστήματα δικτύου και πληροφοριών και τους χρήστες τους·

β) συνδέουν την ταυτότητα των χρηστών με ένα μόνο πρόσωπο·

γ) διασφαλίζουν την εποπτεία των ταυτοτήτων των συστημάτων δικτύου και πληροφοριών·

δ) εφαρμόζουν την καταγραφή για τη διαχείριση ταυτοτήτων.

11.5.3. Οι σχετικές οντότητες επιτρέπουν τις ταυτότητες που αποδίδονται σε πολλαπλά πρόσωπα, όπως κοινές ταυτότητες, μόνον εφόσον είναι απαραίτητες για επιχειρηματικούς ή επιχειρησιακούς λόγους και υπόκεινται σε ρητή διαδικασία έγκρισης και τεκμηρίωση. Οι σχετικές οντότητες λαμβάνουν υπόψη τις ταυτότητες που αποδίδονται σε πολλαπλά πρόσωπα στο πλαίσιο διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας που αναφέρεται στο σημείο 2.1.

11.5.4. Οι σχετικές οντότητες αξιολογούν τακτικά τις ταυτότητες των συστημάτων δικτύου και πληροφοριών και των χρηστών τους και, εάν δεν είναι πλέον αναγκαίο, απενεργοποιούν τις ταυτότητες χωρίς καθυστέρηση.

11.6. *Επαλήθευση ταυτότητας*

11.6.1. Οι σχετικές οντότητες εφαρμόζουν ασφαλείς διαδικασίες και τεχνολογίες επαλήθευσης ταυτότητας με βάση τους περιορισμούς πρόσβασης και την πολιτική ελέγχου πρόσβασης.

11.6.2. Για τον σκοπό αυτό, οι σχετικές οντότητες:

α) διασφαλίζουν ότι η ισχύς της επαλήθευσης ταυτότητας είναι κατάλληλη για την ταξινόμηση του πάγιου στοιχείου στο οποίο παρέχεται πρόσβαση·

β) ελέγχουν την κατανομή στους χρήστες και τη διαχείριση απόρρητων πληροφοριών επαλήθευσης ταυτότητας μέσω διαδικασίας που διασφαλίζει την εμπιστευτικότητα των πληροφοριών, συμπεριλαμβανομένης της παροχής συμβουλών στο προσωπικό σχετικά με τον κατάλληλο χειρισμό των πληροφοριών επαλήθευσης ταυτότητας·

γ) απαιτούν την αλλαγή των διαπιστευτηρίων επαλήθευσης ταυτότητας στην αρχή, σε προκαθορισμένα χρονικά διαστήματα και εφόσον υπάρχουν υπόνοιες ότι τα διαπιστευτήρια παραβιάστηκαν·

δ) απαιτούν την επαναφορά των διαπιστευτηρίων επαλήθευσης ταυτότητας και τον αποκλεισμό των χρηστών μετά από προκαθορισμένο αριθμό ανεπιτυχών προσπαθειών σύνδεσης·

ε) τερματίζουν τις ανενεργές συνεδρίες μετά από προκαθορισμένη περίοδο αδράνειας· και

στ) απαιτούν χωριστά διαπιστευτήρια για την πρόσβαση σε προνομιακή πρόσβαση ή διοικητικούς λογαριασμούς.

11.6.3. Οι σχετικές οντότητες χρησιμοποιούν, στον βαθμό που αυτό είναι εφικτό, σύγχρονες μεθόδους επαλήθευσης ταυτότητας, σύμφωνα με τον σχετικό εκτιμώμενο κίνδυνο και την ταξινόμηση του πάγιου στοιχείου στο οποίο παρέχεται πρόσβαση, καθώς και μοναδικές πληροφορίες επαλήθευσης ταυτότητας.

11.6.4. Οι σχετικές οντότητες αξιολογούν τις διαδικασίες και τις τεχνολογίες επαλήθευσης ταυτότητας σε προγραμματισμένα χρονικά διαστήματα.

11.7. *Πολυπαραγοντική επαλήθευση ταυτότητας*

11.7.1. Οι σχετικές οντότητες διασφαλίζουν ότι οι χρήστες ταυτοποιούνται με πολλαπλούς παράγοντες επαλήθευσης ταυτότητας ή μηχανισμούς συνεχούς επαλήθευσης ταυτότητας για την πρόσβαση στα συστήματα δικτύου και πληροφοριών των σχετικών οντοτήτων, κατά περίπτωση, σύμφωνα με την ταξινόμηση του πάγιου στοιχείου στο οποίο παρέχεται πρόσβαση.

11.7.2. Οι σχετικές οντότητες διασφαλίζουν ότι η ισχύς της επαλήθευσης ταυτότητας είναι κατάλληλη για την ταξινόμηση του πάγιου στοιχείου στο οποίο παρέχεται πρόσβαση.

12. **Διαχείριση πάγιων στοιχείων [άρθρο 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555]**

12.1. *Ταξινόμηση πάγιων στοιχείων*

12.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες καθορίζουν τα επίπεδα ταξινόμησης όλων των πάγιων στοιχείων, συμπεριλαμβανομένων των πληροφοριών, στο πεδίο εφαρμογής των οικείων συστημάτων δικτύου και πληροφοριών για το απαιτούμενο επίπεδο προστασίας.

12.1.2. Για τους σκοπούς του σημείου 12.1.1., οι σχετικές οντότητες:

α) θεσπίζουν σύστημα επιπέδων ταξινόμησης για τα πάγια στοιχεία·

β) συνδέουν όλα τα πάγια στοιχεία με επίπεδο ταξινόμησης, με βάση τις απαιτήσεις εμπιστευτικότητας, ακεραιότητας, αυθεντικότητας και διαθεσιμότητας, ώστε να υποδεικνύουν την προστασία που απαιτείται ανάλογα με την ευαισθησία, την κρισιμότητα, τον κίνδυνο και την επιχειρηματική αξία τους·

γ) ευθυγραμμίζουν τις απαιτήσεις διαθεσιμότητας των πάγιων στοιχείων με τους στόχους παράδοσης και αποκατάστασης που καθορίζονται στα σχέδια επιχειρησιακής συνέχειας και αποκατάστασης έπειτα από καταστροφή.

12.1.3. Οι σχετικές οντότητες διενεργούν περιοδικές αξιολογήσεις των επιπέδων ταξινόμησης των πάγιων στοιχείων και τα επικαιροποιούν, κατά περίπτωση.

12.2. *Χειρισμός πάγιων στοιχείων*

12.2.1. Οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική για τον ορθό χειρισμό πάγιων στοιχείων, συμπεριλαμβανομένων των πληροφοριών, σύμφωνα με την οικεία πολιτική για την ασφάλεια δικτύου και πληροφοριών, και κοινοποιούν την πολιτική για τον ορθό χειρισμό πάγιων στοιχείων σε οποιονδήποτε χρησιμοποιεί ή χειρίζεται πάγια στοιχεία.

12.2.2. Η πολιτική αυτή:

α) καλύπτει ολόκληρο τον κύκλο ζωής των πάγιων στοιχείων, συμπεριλαμβανομένων της απόκτησης, της χρήσης, της αποθήκευσης, της μεταφοράς και της διάθεσης·

β) προβλέπει κανόνες για την ασφαλή χρήση, την ασφαλή αποθήκευση, την ασφαλή μεταφορά και την ανεπανόρθωτη διαγραφή και καταστροφή των πάγιων στοιχείων·

γ) προβλέπει ότι η μεταβίβαση πραγματοποιείται με ασφαλή τρόπο, ανάλογα με το είδος του προς μεταβίβαση πάγιου στοιχείου.

12.2.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την εν λόγω πολιτική σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

12.3. *Πολιτική για τα αφαιρούμενα μέσα*

12.3.1. Οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν πολιτική για τη διαχείριση των αφαιρούμενων μέσων αποθήκευσης και την κοινοποιούν στους υπαλλήλους τους και σε τρίτα μέρη που χειρίζονται αφαιρούμενα μέσα αποθήκευσης στις εγκαταστάσεις των σχετικών οντοτήτων ή σε άλλες τοποθεσίες όπου τα αφαιρούμενα μέσα είναι συνδεδεμένα με τα συστήματα δικτύου και πληροφοριών των σχετικών οντοτήτων.

12.3.2. Η πολιτική αυτή:

α) προβλέπει τεχνική απαγόρευση της σύνδεσης αφαιρούμενων μέσων, εκτός εάν υπάρχει οργανωτικός λόγος για τη χρήση τους·

β) προβλέπει την απενεργοποίηση της αυτοεκτέλεσης από τα εν λόγω μέσα και τη σάρωση των μέσων για κακόβουλο κώδικα πριν από τη χρήση τους στα συστήματα των σχετικών οντοτήτων·

γ) προβλέπει μέτρα για τον έλεγχο και την προστασία φορητών συσκευών αποθήκευσης που περιέχουν δεδομένα κατά τη διάρκεια της διαμετακόμισης και της αποθήκευσης·

δ) κατά περίπτωση, προβλέπει μέτρα για τη χρήση τεχνικών κρυπτογραφίας για την προστασία των δεδομένων σε αφαιρούμενα μέσα αποθήκευσης.

12.3.3. Οι σχετικές οντότητες αξιολογούν και, κατά περίπτωση, επικαιροποιούν την εν λόγω πολιτική σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση εκδήλωσης σημαντικών περιστατικών ή σημαντικών αλλαγών στις λειτουργίες ή στους κινδύνους.

12.4. *Κατάλογος απογραφής πάγιων στοιχείων*

12.4.1. Οι σχετικές οντότητες καταρτίζουν και διατηρούν πλήρη, ακριβή, επικαιροποιημένο και συνεπή κατάλογο απογραφής των οικείων πάγιων στοιχείων. Καταγράφουν τις μεταβολές των εγγραφών στον κατάλογο απογραφής με ανιχνεύσιμο τρόπο.

12.4.2. Ο βαθμός λεπτομέρειας της απογραφής πάγιων στοιχείων είναι σε επίπεδο κατάλληλο για τις ανάγκες των σχετικών οντοτήτων. Ο κατάλογος απογραφής περιλαμβάνει τα ακόλουθα:

α) τη λίστα των λειτουργιών και των υπηρεσιών και την περιγραφή τους·

β) τη λίστα των συστημάτων δικτύου και πληροφοριών και άλλων συναφών πάγιων στοιχείων που υποστηρίζουν τις λειτουργίες και τις υπηρεσίες των σχετικών οντοτήτων.

12.4.3. Οι σχετικές οντότητες αξιολογούν και επικαιροποιούν τακτικά τον κατάλογο απογραφής και τα οικεία πάγια στοιχεία και τεκμηριώνουν το ιστορικό των μεταβολών.

12.5. *Κατάθεση, επιστροφή ή διαγραφή πάγιων στοιχείων κατά τη λήξη της απασχόλησης*

Οι σχετικές οντότητες θεσπίζουν, υλοποιούν και εφαρμόζουν διαδικασίες που διασφαλίζουν ότι τα πάγια στοιχεία τους που τελούν υπό τη φύλαξη του προσωπικού κατατίθενται, επιστρέφονται ή διαγράφονται κατά τη λήξη της απασχόλησής τους και τεκμηριώνουν την κατάθεση, την επιστροφή και τη διαγραφή των εν λόγω πάγιων στοιχείων. Όταν δεν είναι δυνατή η κατάθεση, η επιστροφή ή η διαγραφή πάγιων στοιχείων, οι σχετικές οντότητες διασφαλίζουν ότι τα πάγια στοιχεία δεν μπορούν πλέον να έχουν πρόσβαση στα συστήματα δικτύου και πληροφοριών των σχετικών οντοτήτων σύμφωνα με το σημείο 12.2.2.

13. **Περιβαλλοντική και φυσική ασφάλεια [άρθρο 21 παράγραφος 2 στοιχεία γ), ε) και θ) της οδηγίας (ΕΕ) 2022/2555]**

13.1. *Υποστηρικτικές υπηρεσίες κοινής ωφελείας*

13.1.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο γ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες αποτρέπουν την απώλεια, τη ζημία ή την έκθεση σε κίνδυνο των συστημάτων δικτύου και πληροφοριών ή τη διακοπή της λειτουργίας τους λόγω αστοχίας και διατάραξης των υποστηρικτικών υπηρεσιών κοινής ωφελείας.

13.1.2. Για τον σκοπό αυτό, οι σχετικές οντότητες, κατά περίπτωση:

α) προστατεύουν τις εγκαταστάσεις από αστοχίες στην ηλεκτροδότηση και άλλες διαταράξεις που προκαλούνται από αστοχία των υποστηρικτικών υπηρεσιών κοινής ωφελείας, όπως η ηλεκτρική ενέργεια, οι τηλεπικοινωνίες, η ύδρευση, το αέριο, η αποχέτευση, ο εξαερισμός και ο κλιματισμός·

β) εξετάζουν το ενδεχόμενο χρήσης εφεδρικών υπηρεσιών κοινής ωφελείας·

γ) προστατεύουν τις υπηρεσίες κοινής ωφελείας για την ηλεκτρική ενέργεια και τις τηλεπικοινωνίες, οι οποίες μεταφέρουν δεδομένα ή τροφοδοτούν συστήματα δικτύου και πληροφοριών, από υποκλοπές και ζημίες·

δ) παρακολουθούν τις υπηρεσίες κοινής ωφέλειας που αναφέρονται στο στοιχείο γ) και αναφέρουν στο αρμόδιο εσωτερικό ή εξωτερικό προσωπικό συμβάντα εκτός των ελάχιστων και μέγιστων ορίων ελέγχου που αναφέρονται στο σημείο 13.2.2. στοιχείο β) και επηρεάζουν τις υπηρεσίες κοινής ωφέλειας·

ε) συνάπτουν συμβάσεις για προμήθειες έκτακτης ανάγκης με τις αντίστοιχες υπηρεσίες, όπως καύσιμα για την παροχή ηλεκτρικής ενέργειας έκτακτης ανάγκης·

στ) εξασφαλίζουν συνεχή αποτελεσματικότητα, παρακολουθούν, συντηρούν και ελέγχουν την τροφοδοσία των συστημάτων δικτύου και πληροφοριών που απαιτείται για τη λειτουργία της προσφερόμενης υπηρεσίας, ιδίως όσον αφορά τον έλεγχο της ηλεκτρικής ενέργειας, της θερμοκρασίας και της υγρασίας, των τηλεπικοινωνιών και της σύνδεσης στο διαδίκτυο.

13.1.3. Οι σχετικές οντότητες ελέγχουν, αξιολογούν και, κατά περίπτωση, επικαιροποιούν τα μέτρα προστασίας σε τακτική βάση ή έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους.

13.2. *Προστασία από φυσικές και περιβαλλοντικές απειλές*

13.2.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο ε) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες προλαμβάνουν ή μειώνουν τις συνέπειες συμβάντων που προέρχονται από φυσικές και περιβαλλοντικές απειλές, όπως φυσικές καταστροφές και άλλες εκούσιες ή ακούσιες απειλές, με βάση τα αποτελέσματα της εκτίμησης κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1.

13.2.2. Για τον σκοπό αυτό, οι σχετικές οντότητες, κατά περίπτωση:

α) σχεδιάζουν και εφαρμόζουν μέτρα προστασίας από φυσικές και περιβαλλοντικές απειλές·

β) καθορίζουν ελάχιστα και μέγιστα όρια ελέγχου για φυσικές και περιβαλλοντικές απειλές·

γ) παρακολουθούν τις περιβαλλοντικές παραμέτρους και αναφέρουν στο αρμόδιο εσωτερικό ή εξωτερικό προσωπικό συμβάντα εκτός των ελάχιστων και μέγιστων ορίων ελέγχου που αναφέρονται στο στοιχείο β).

13.2.3. Οι σχετικές οντότητες ελέγχουν, αξιολογούν και, κατά περίπτωση, επικαιροποιούν τα μέτρα προστασίας από φυσικές και περιβαλλοντικές απειλές σε τακτική βάση ή έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους.

13.3. *Περίμετρος ασφαλείας και έλεγχος φυσικής πρόσβασης*

13.3.1. Για τους σκοπούς του άρθρου 21 παράγραφος 2 στοιχείο θ) της οδηγίας (ΕΕ) 2022/2555, οι σχετικές οντότητες αποτρέπουν και παρακολουθούν τη μη εξουσιοδοτημένη φυσική πρόσβαση, τις ζημίες και τις παρεμβολές στα οικεία συστήματα δικτύου και πληροφοριών.

13.3.2. Για τον σκοπό αυτό, οι σχετικές οντότητες:

α) με βάση την εκτίμηση κινδύνου που διενεργείται σύμφωνα με το σημείο 2.1., καθορίζουν και χρησιμοποιούν περιμέτρους ασφαλείας για την προστασία περιοχών όπου βρίσκονται συστήματα δικτύου και πληροφοριών και άλλα συναφή πάγια στοιχεία·

β) προστατεύουν τις περιοχές που αναφέρονται στο στοιχείο α) με κατάλληλους ελέγχους εισόδου και σημεία πρόσβασης·

γ) σχεδιάζουν και εφαρμόζουν φυσική ασφάλεια για γραφεία, αίθουσες και εγκαταστάσεις·

δ) παρακολουθούν συνεχώς τις εγκαταστάσεις τους για μη εξουσιοδοτημένη φυσική πρόσβαση.

13.3.3. Οι σχετικές οντότητες ελέγχουν, αξιολογούν και, κατά περίπτωση, επικαιροποιούν τα μέτρα ελέγχου φυσικής πρόσβασης σε τακτική βάση ή έπειτα από σημαντικά περιστατικά ή σημαντικές αλλαγές στις λειτουργίες ή στους κινδύνους.