ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 17.10.2024
C(2024) 7151 final

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) …/... ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 17.10.2024

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)

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) …/... ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 17.10.2024

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

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

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 319 401, 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.

(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

[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).

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.

(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.

[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

(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.

   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.

απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Άρθρο 3

Σημαντικά περιστατικά

1. Ένα περιστατικό θεωρείται σημαντικό για τους σκοπούς του άρθρου 23 παράγραφος 3 της οδηγίας 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, 17.10.2024

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

[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).