Οδηγία NIS2: νέοι κανόνες για την κυβερνοασφάλεια των συστημάτων δικτύου και πληροφοριών

Η ασφάλεια στον κυβερνοχώρο περιλαμβάνει την προστασία των **συστημάτων δικτύου και πληροφοριών** (NIS), των χρηστών τους και άλλων θιγόμενων ατόμων από συμβάντα και απειλές στον κυβερνοχώρο. Για την αντιμετώπιση της αυξημένης έκθεσης της Ευρώπης σε κυβερνοαπειλές, η οδηγία 2022/2555, γνωστή και ως NIS2, αντικατέστησε (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555) την προκάτοχό της, την οδηγία 2016/1148 ή την οδηγία NIS1. Το NIS2 αυξάνει το κοινό επίπεδο φιλοδοξίας της ΕΕ για την ασφάλεια στον κυβερνοχώρο, μέσω ενός ευρύτερου πεδίου εφαρμογής, σαφέστερων κανόνων και ισχυρότερων εργαλείων εποπτείας. Απαιτεί από τα κράτη μέλη να **ενισχύσουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας**, εισάγοντας παράλληλα μέτρα διαχείρισης κινδύνων και απαιτήσεις υποβολής εκθέσεων σε οντότητες από περισσότερους τομείς και θεσπίζοντας κανόνες για τη συνεργασία, την ανταλλαγή πληροφοριών, την εποπτεία και την επιβολή των μέτρων κυβερνοασφάλειας.

Η οδηγία ορίζει ότι κάθε κράτος μέλος πρέπει να εγκρίνει εθνική στρατηγική για την κυβερνοασφάλεια, η οποία περιλαμβάνει πολιτικές για την ασφάλεια της αλυσίδας εφοδιασμού, τη διαχείριση τρωτών σημείων και την εκπαίδευση και ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας. Τα κράτη μέλη πρέπει επίσης να καταρτίζουν και να επικαιροποιούν τακτικά κατάλογο των φορέων εκμετάλλευσης βασικών υπηρεσιών, διασφαλίζοντας ότι οι εν λόγω φορείς συμμορφώνονται με τις απαιτήσεις της οδηγίας.

Εκτός από τους τομείς που καλύπτονται ήδη από την ΑΔΠ 1, όπως η ενέργεια, οι μεταφορές, η υγειονομική περίθαλψη, η χρηματοδότηση, η διαχείριση των υδάτων και οι ψηφιακές υποδομές, οι κανόνες αυτοί ισχύουν για τους παρόχους δημόσιων υπηρεσιών ηλεκτρονικών επικοινωνιών, περισσότερες ψηφιακές υπηρεσίες, όπως οι κοινωνικές πλατφόρμες, η διαχείριση λυμάτων και αποβλήτων, η κατασκευή προϊόντων κρίσιμης σημασίας, οι ταχυδρομικές υπηρεσίες και οι υπηρεσίες ταχυμεταφοράς, η δημόσια διοίκηση, τόσο σε κεντρικό όσο και σε περιφερειακό επίπεδο ή στο διάστημα. Κατά κανόνα, οι μεσαίες και μεγάλες οντότητες σε αυτούς τους κρίσιμους τομείς θα πρέπει να λαμβάνουν κατάλληλα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και να ενημερώνουν τις αρμόδιες εθνικές αρχές για σημαντικά συμβάντα. Πρόκειται για περιστατικά που θα μπορούσαν να προκαλέσουν σημαντική αναστάτωση ή ζημιά.

Η οδηγία περιλαμβάνει επίσης διατάξεις για την εποπτεία, την επιβολή και τις εθελοντικές αξιολογήσεις από ομοτίμους για την ενίσχυση της αμοιβαίας εμπιστοσύνης και των ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την ΕΕ. Εισάγει επίσης τη λογοδοσία της ανώτατης διοίκησης για τη μη συμμόρφωση με τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, φέρνοντας έτσι την κυβερνοασφάλεια υπόψη της αίθουσας του διοικητικού συμβουλίου.

Η οδηγία δημιουργεί ένα δίκτυο ομάδων αντιμετώπισης συμβάντων ασφάλειας υπολογιστών (CSIRT) (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network) για την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές και την αντιμετώπιση συμβάντων. Οι ομάδες αυτές είναι ζωτικής σημασίας για τη διατήρηση της επίγνωσης της κατάστασης και την παροχή βοήθειας. Για τη διαχείριση συμβάντων ή κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας, η οδηγία δημιουργεί το ευρωπαϊκό δίκτυο οργανισμών σύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe) (https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone). Το δίκτυο αυτό υποστηρίζει τη συντονισμένη διαχείριση και διασφαλίζει την τακτική ανταλλαγή πληροφοριών μεταξύ των κρατών μελών και των θεσμικών οργάνων της ΕΕ σε περίπτωση συμβάντων και κρίσεων μεγάλης κλίμακας.

Παράλληλα, η ομάδα συνεργασίας NIS (https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group) είναι μια πλατφόρμα που δημιουργήθηκε από την οδηγία NIS για τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών της ΕΕ, της Ευρωπαϊκής Επιτροπής και του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια (ENISA). Η ομάδα δημοσιεύει μη δεσμευτικές κατευθυντήριες γραμμές και συστάσεις για την υποστήριξη της εφαρμογής της οδηγίας NIS.

Ιστορικό

Η NIS 1 (οδηγία 2016/1148) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148) ήταν η πρώτη ολοκληρωμένη νομοθεσία της ΕΕ που αποσκοπούσε στην ενίσχυση της κυβερνοασφάλειας των συστημάτων δικτύου και πληροφοριών για τη διασφάλιση των υπηρεσιών ζωτικής σημασίας για την οικονομία και την κοινωνία της ΕΕ. Τον Δεκέμβριο του 2020, η Επιτροπή πρότεινε την αναθεώρηση της NIS 1, με αποτέλεσμα την έγκριση της NIS 2, η οποία τέθηκε σε ισχύ τον Ιανουάριο του 2023. Τα κράτη μέλη είχαν προθεσμία έως τις 17 Οκτωβρίου 2024 για να μεταφέρουν την οδηγία NIS2 στο εθνικό τους δίκαιο. Το NIS 2 καταργήθηκε το NIS1 από τις 18 Οκτωβρίου 2024.

Η Επιτροπή κίνησε διαδικασίες επί παραβάσει

(https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en) στέλνοντας προειδοποιητικές επιστολές σε 23 κράτη μέλη για μη πλήρη μεταφορά της οδηγίας NIS2 στο εθνικό δίκαιο έως (https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive) τη λήξη της προθεσμίας της 17ης Οκτωβρίου 2024. Τα κράτη μέλη πρέπει να ανταποκριθούν και να ολοκληρώσουν τη μεταφορά της οδηγίας στο εθνικό δίκαιο. Εάν δεν το πράξουν, η Επιτροπή μπορεί να εκδώσει αιτιολογημένη γνώμη, η οποία αποτελεί επίσημο αίτημα συμμόρφωσης με το δίκαιο της ΕΕ. Η συνεχιζόμενη μη συμμόρφωση θα μπορούσε τελικά να οδηγήσει στην παραπομπή της υπόθεσης στο Δικαστήριο της Ευρωπαϊκής Ένωσης, το οποίο μπορεί να επιβάλει οικονομικές κυρώσεις.
