Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων — Ερωτήσεις και απαντήσεις

Βρυξέλλες, 16 Δεκεμβρίου 2020

Ευρετήριο

1. Στρατηγική της ΕΕ για την κυβερνοασφάλεια για την ψηφιακή δεκαετία

Τι αφορά η νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια;

Η νέα στρατηγική για την κυβερνοασφάλεια έχει ως στόχο να διαφυλάξει ένα παγκόσμιο και ανοικτό διαδίκτυο, αξιοποιώντας και ενισχύοντας όλα τα εργαλεία και τους πόρους για την εγγύηση της ασφάλειας και την προστασία των ευρωπαϊκών αξιών και των θεμελιωδών δικαιωμάτων όλων.

Τι νέο υπάρχει σε αυτήν τη στρατηγική για την κυβερνοασφάλεια;

Στις στρατηγικές πρωτοβουλίες περιλαμβάνονται:

- Κυβερνοασπίδα σε ολόκληρη την ΕΕ, αποτελούμενη από κέντρα επιχειρήσεων ασφάλειας που χρησιμοποιούν τεχνητή νοημοσύνη και μηχανομάθηση για τον εντοπισμό έγκαιρων ενδείξεων επικείμενης κυβερνοεπίθεσης και καθιστούν δυνατή την ανάληψη δράσης πριν από την πρόκληση βλάβης
- Κοινή Μονάδα Κυβερνοχώρου που θα φέρει σε επαφή όλες τις κοινότητες κυβερνοασφάλειας για την ανταλλαγή γνώσεων σχετικά με απειλές και τη συλλογική αντιμετώπιση περιστατικών και απειλών
- Ευρωπαϊκές λύσεις για την ενίσχυση της ασφάλειας του διαδικτύου σε παγκόσμιο επίπεδο, συμπεριλαμβανομένης μιας δημόσιας υπηρεσίας επίλυσης DNS (DNS Resolver Service) της ΕΕ
- Κανονιστική ρύθμιση για να διασφαλιστεί το διαδίκτυο των ασφαλών πραγμάτων
- Ισχυρότερη εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο με σκοπό την πρόληψη, την αποτροπή και την αντιμετώπιση κυβερνοεπιθέσεων
- Ενισχυμένη συνεργασία στον τομέα της κυβερνοάμυνας, ιδίως μέσω της επανεξέτασης του πλαισίου πολιτικής της άμυνας στον κυβερνοχώρο
- Πρόγραμμα δράσης στα Ηνωμένα Έθνη για την αντιμετώπιση του ζητήματος της διεθνούς ασφάλειας στον κυβερνοχώρο
- Περισσότεροι και ισχυρότεροι κυβερνοδιάλογοι με τρίτες χώρες και περιφερειακούς και διεθνείς οργανισμούς, συμπεριλαμβανομένου του ΝΑΤΟ
- Ένα θεματολόγιο για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο και ένα διοργανικό συμβούλιο για την ανάπτυξη των ικανοτήτων της ΕΕ στον κυβερνοχώρο με σκοπό να αυξηθεί η αποτελεσματικότητα και η αποδοτικότητα της ανάπτυξης των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο.

Τι σημαίνει ο όρος «κυβερνοασπίδα»;

Η ΕΕ χρειάζεται ένα ευέλικτο μέσο για τον εντοπισμό και την αντιμετώπιση των κυβερνοεπιθέσεων.

Επί του παρόντος, τα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) βοηθούν τους ενδιαφερόμενους φορείς του κλάδου και τις δημόσιες αρχές να ανταλλάσσουν πληροφορίες σχετικά με απειλές. Ωστόσο, πρέπει επίσης να παρακολουθούμε συνεχώς τα δίκτυα και τα συστήματα υπολογιστών για τον εντοπισμό εισβολών και ανωμαλιών σε πραγματικό χρόνο.

Πολλές ιδιωτικές εταιρείες, δημόσιοι οργανισμοί και εθνικές αρχές το πράττουν αυτό μέσω κέντρων επιχειρήσεων ασφάλειας.

Πρόκειται για εξαιρετικά απαιτητική και ταχύρρυθμη εργασία και, γι' αυτόν τον λόγο, η τεχνητή νοημοσύνη και ιδίως οι τεχνικές μηχανομάθησης μπορούν να παράσχουν πολύτιμη στήριξη στους επαγγελματίες του τομέα.

Η Επιτροπή προτείνει να δημιουργηθεί δίκτυο κέντρων επιχειρήσεων ασφάλειας σε ολόκληρη την ΕΕ και να στηριχθεί η βελτίωση των υφιστάμενων κέντρων, καθώς και η ίδρυση νέων. Θα στηρίξει επίσης την κατάρτιση και την ανάπτυξη δεξιοτήτων του προσωπικού που διαχειρίζεται τα κέντρα αυτά. Το εν λόγω δίκτυο θα παρέχει έγκαιρες προειδοποιήσεις σχετικά με περιστατικά κυβερνοασφάλειας στις αρχές και σε όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένης της Κοινής Μονάδας Κυβερνοχώρου, σαν ένα πλέγμα παρατηρητών.

Τι είναι η Κοινή Μονάδα Κυβερνοχώρου και γιατί τη χρειαζόμαστε;

Η πρόεδρος της Επιτροπής ζήτησε τη σύσταση Κοινής Μονάδας Κυβερνοχώρου στις πολιτικές κατευθύνσεις της το 2019.

Θα καλύψει τα κενά και θα δώσει σημαντική ώθηση στην ενίσχυση της υφιστάμενης συνεργασίας μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ και των αρχών των κρατών μελών σε περίπτωση που χρειαστεί διάφορες κυβερνοκοινότητες να συνεργαστούν στενά για την αντιμετώπιση σοβαρών διασυνοριακών περιστατικών ή απειλών στον κυβερνοχώρο.

Πρώτον, θα παρέχει έναν χώρο συνεργασίας για τις μη στρατιωτικές, διπλωματικές, αστυνομικές και αμυντικές κοινότητες κυβερνοασφάλειας.

Δεύτερον, θα παρέχει στους ενδιαφερόμενους φορείς στον τομέα της κυβερνοασφάλειας ένα σημείο επαφής για την ανταλλαγή πληροφοριών σχετικά με απειλές.

Η Επιτροπή δεσμεύεται να αυξήσει τους πόρους και τις ικανότητες που διατίθενται για την κυβερνοασφάλεια σε επίπεδο ΕΕ, ώστε να αντιμετωπιστούν οι εξελισσόμενες απειλές και να χρησιμοποιηθούν οι εν λόγω πρόσθετοι πόροι ως συμβολή στο έργο της Κοινής Μονάδας Κυβερνοχώρου.

Ποιο είναι το ύψος των επενδύσεων που έχουν προγραμματιστεί για την κυβερνοασφάλεια;

Στο πολυετές δημοσιονομικό πλαίσιο 2021-2027 προβλέπεται ενωσιακή χρηματοδότηση για την κυβερνοασφάλεια στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» και για την έρευνα στον τομέα της κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη», με ιδιαίτερη έμφαση στη στήριξη των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ)· η χρηματοδότηση αυτή θα μπορούσε να ανέλθει συνολικά σε 2 δισ. EUR συν τις επενδύσεις των κρατών μελών και του κλάδου.

Οι επενδύσεις σε ολόκληρη την αλυσίδα παροχής ψηφιακής τεχνολογίας αναμένεται να ανέλθουν τουλάχιστον στο 20 % —ποσοστό που ισοδυναμεί με 134,5 δισ. EUR— του Μηχανισμού Ανάκαμψης και Ανθεκτικότητας ύψους 672,5 δισ. EUR ο οποίος αποτελείται από επιχορηγήσεις και δάνεια.

Το Ευρωπαϊκό Ταμείο Άμυνας (EDF) θα στηρίξει ευρωπαϊκές λύσεις κυβερνοάμυνας.

Πώς θα προωθήσει η ΕΕ έναν παγκόσμιο, ανοικτό, σταθερό και ασφαλή κυβερνοχώρο;

Η ΕΕ θα εντείνει τις εργασίες της για την ενίσχυση της παγκόσμιας τάξης που βασίζεται σε κανόνες, για την προώθηση της διεθνούς ασφάλειας και σταθερότητας στον κυβερνοχώρο, και για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στο διαδίκτυο.

Θα προωθήσει διεθνείς κανόνες και πρότυπα που αντικατοπτρίζουν αυτές τις βασικές αξίες της ΕΕ, συνεργαζόμενη με τους διεθνείς εταίρους της στα Ηνωμένα Έθνη και σε άλλα σχετικά φόρουμ.

Επιπλέον, η ΕΕ θα ενισχύσει περαιτέρω την εργαλειοθήκη της για τη διπλωματία στον κυβερνοχώρο και θα εντείνει τις προσπάθειες ανάπτυξης ικανοτήτων στον κυβερνοχώρο σε χώρες-εταίρους με την εκπόνηση ενός θεματολογίου για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο.

Θα εντατικοποιηθούν οι κυβερνοδιάλογοι με τρίτες χώρες, περιφερειακούς και διεθνείς οργανισμούς, καθώς και με την πολυσυμμετοχική κοινότητα.

2. Πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση («NIS 2»)

Γιατί προτείνει η Επιτροπή μια νέα οδηγία NIS;

Ο ψηφιακός μετασχηματισμός της κοινωνίας, ο οποίος εντάθηκε σε μεγάλο βαθμό κατά τη διάρκεια της κρίσης του κορονοϊού, έχει διευρύνει το τοπίο των απειλών και δημιουργεί νέες προκλήσεις, οι οποίες απαιτούν προσαρμοσμένες και καινοτόμες απαντήσεις.

Η Επιτροπή, για να μπορέσει να αναλύσει τον αντίκτυπο και να εντοπίσει τις ελλείψεις της ισχύουσας οδηγίας NIS, διεξήγαγε εκτενή διαβούλευση με τα ενδιαφερόμενα μέρη και προσδιόρισε τα ακόλουθα κύρια ζητήματα: 1) ανεπαρκές επίπεδο κυβερνοανθεκτικότητας των επιχειρήσεων που δραστηριοποιούνται στην ΕΕ· 2) διαφορές όσον αφορά την ανθεκτικότητα μεταξύ κρατών μελών και τομέων· και 3) ανεπαρκής κοινή αντίληψη των κυριότερων απειλών και προκλήσεων μεταξύ των κρατών μελών και έλλειψη κοινής αντιμετώπισης κρίσεων.

Ποια είναι τα βασικά στοιχεία της πρότασης της Επιτροπής;

Η νέα πρόταση της Επιτροπής αποσκοπεί στην αντιμετώπιση των ελλείψεων της προηγούμενης οδηγίας NIS.

Η πρόταση της Επιτροπής διευρύνει το πεδίο εφαρμογής της ισχύουσας οδηγίας NIS, προσθέτοντας νέους τομείς με βάση την κρισιμότητά τους για την οικονομία και την κοινωνία, και εισάγοντας ένα σαφές ανώτατο όριο μεγέθους — που σημαίνει ότι όλες οι μεσαίες και μεγάλες επιχειρήσεις σε επιλεγμένους τομείς θα συμπεριληφθούν στο πεδίο εφαρμογής της. Ταυτόχρονα, αφήνει κάποια ευελιξία στα κράτη μέλη να προσδιορίζουν μικρότερες οντότητες με προφίλ υψηλού κινδύνου ασφάλειας.

Η πρόταση καταργεί επίσης τη διάκριση μεταξύ φορέων εκμετάλλευσης βασικών υπηρεσιών και παρόχων ψηφιακών υπηρεσιών.

Η πρόταση ενισχύει και εξορθολογίζει τις απαιτήσεις ασφάλειας και κοινοποίησης για τις εταιρείες.

Επιπλέον, η Επιτροπή προτείνει να αντιμετωπιστεί το ζήτημα της ασφάλειας των αλυσίδων εφοδιασμού και των σχέσεων με τους προμηθευτές. Σε ευρωπαϊκό επίπεδο, η πρόταση ενισχύει την κυβερνοασφάλεια της αλυσίδας εφοδιασμού για βασικές τεχνολογίες των πληροφοριών και των επικοινωνιών. Τα κράτη μέλη, σε συνεργασία με την Επιτροπή και τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), μπορούν να διενεργούν συντονισμένες εκτιμήσεις κινδύνου για τις κρίσιμες αλυσίδες εφοδιασμού, με βάση την επιτυχημένη προσέγγιση που ακολουθήθηκε στο πλαίσιο της σύστασης της Επιτροπής για την κυβερνοασφάλεια δικτύων 5G.

Η πρόταση εισάγει αυστηρότερα εποπτικά μέτρα για τις εθνικές αρχές, καθώς και αυστηρότερες απαιτήσεις επιβολής, και αποσκοπεί στην εναρμόνιση των καθεστώτων κυρώσεων σε όλα τα κράτη μέλη.

Η πρόταση ενισχύει επίσης τον ρόλο της ομάδας συνεργασίας και αυξάνει την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των αρχών των κρατών μελών.

Ποιους τομείς και ποια είδη οντοτήτων θα καλύπτει η πρόταση της Επιτροπής;

Η πρόταση της Επιτροπής καλύπτει τους ακόλουθους τομείς και υποτομείς:

- **Βασικές οντότητες:** ενέργεια (ηλεκτρική ενέργεια, τηλεθέρμανση και τηλεψύξη, πετρέλαιο, φυσικό αέριο και υδρογόνο)· μεταφορές (αεροπορικές, σιδηροδρομικές, πλωτές και οδικές μεταφορές)· τράπεζες· υποδομές χρηματοπιστωτικών αγορών· υγεία· παρασκευή φαρμακευτικών προϊόντων, συμπεριλαμβανομένων των εμβολίων, και ιατροτεχνολογικών προϊόντων ζωτικής σημασίας· πόσιμο νερό· λύματα· ψηφιακή υποδομή (σημεία ανταλλαγής κίνησης διαδικτύου· πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS)· μητρώα ονομάτων τομέων ανώτατης στάθμης (TLD)· πάροχοι υπηρεσιών νεφοϋπολογιστικής· πάροχοι υπηρεσιών κέντρων δεδομένων· δίκτυα διανομής περιεχομένου· πάροχοι υπηρεσιών εμπιστοσύνης· και δημόσια δίκτυα ηλεκτρονικών επικοινωνιών και υπηρεσίες ηλεκτρονικών επικοινωνιών)· δημόσια διοίκηση· και διάστημα.
- **Σημαντικές οντότητες:** ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών· διαχείριση αποβλήτων· χημικές ουσίες· τρόφιμα· κατασκευή άλλων ιατροτεχνολογικών προϊόντων, υπολογιστών και ηλεκτρονικών ειδών, μηχανολογικού εξοπλισμού, μηχανοκίνητων οχημάτων· και πάροχοι ψηφιακών υπηρεσιών (επιγραμμικές αγορές, επιγραμμικές μηχανές αναζήτησης και πλατφόρμες υπηρεσιών κοινωνικής δικτύωσης).

Ποια είναι τα επόμενα βήματα;

Η πρόταση θα αποτελέσει αντικείμενο διαπραγματεύσεων μεταξύ των συννομοθετών, δηλαδή του Συμβουλίου της Ευρωπαϊκής Ένωσης και του Ευρωπαϊκού Κοινοβουλίου. Μετά την επίτευξη συμφωνίας και την έγκριση της πρότασης, τα κράτη μέλη θα πρέπει να μεταφέρουν την οδηγία NIS 2 στο εθνικό τους δίκαιο εντός 18 μηνών από την έναρξη ισχύος της. Η Επιτροπή πρέπει να επανεξετάζει

περιοδικά την οδηγία και να υποβάλει έκθεση για πρώτη φορά 54 μήνες μετά την έναρξη ισχύος της.

3. Έκθεση σχετικά με τον αντίκτυπο της σύστασης της Επιτροπής για την κυβερνοασφάλεια δικτύων 5G

Ποια είναι τα κύρια πορίσματα της επανεξέτασης της σύστασης της Επιτροπής;

Από την επανεξέταση προκύπτει ότι τα κράτη μέλη εκτίμησαν ιδιαίτερα τη διαδικασία που ξεκίνησε με τη σύσταση της Επιτροπής του Μαρτίου του 2019 για την κυβερνοασφάλεια δικτύων 5G και επιθυμούν να συνεχίσουν τις συντονισμένες εργασίες για το θέμα αυτό σε επίπεδο ΕΕ. Η εργαλειοθήκη μέτρων μετριασμού εκλαμβάνεται ως **χρήσιμο μέσο** που παρέχει ολοκληρωμένη καθοδήγηση, με βάση τους κινδύνους και αντικειμενική μεθοδολογία.

Από την επανεξέταση προκύπτει επίσης ότι τα περισσότερα κράτη μέλη έχουν σημειώσει **περαιτέρω πρόοδο** όσον αφορά την εφαρμογή των μέτρων της εργαλειοθήκης σε εθνικό επίπεδο μετά τη δημοσίευση της έκθεσης προόδου τον Ιούλιο του 2020. Μολονότι οι εθνικές διαδικασίες βρίσκονται ακόμη σε εξέλιξη, τα περισσότερα κράτη μέλη βρίσκονται σε καλό δρόμο όσον αφορά την ολοκλήρωσή τους κατά τους προσεχείς μήνες. Ωστόσο, υπάρχουν ορισμένες διαφορές μεταξύ των επιμέρους μέτρων.

Πού βρίσκονται τα κράτη μέλη όσον αφορά την εφαρμογή των μέτρων της εργαλειοθήκης;

Μετά τη δημοσίευση της έκθεσης προόδου τον Ιούλιο του 2020, τα περισσότερα κράτη μέλη σημείωσαν περαιτέρω πρόοδο όσον αφορά την εφαρμογή των διαφόρων μέτρων της εργαλειοθήκης σε εθνικό επίπεδο. Συνολικά, σχεδόν όλα τα κράτη μέλη εκτίμησαν ότι θα ολοκληρώσουν την εν εξελίξει διαδικασία εφαρμογής έως τα **μέσα του 2021**. Ωστόσο, ορισμένοι τομείς απαιτούν ιδιαίτερη προσοχή και ορισμένα κράτη μέλη εξακολουθούν να μην έχουν κοινοποιήσει σαφή σχέδια όσον αφορά ορισμένα μέτρα.

Συγκεκριμένα:

- Οι **ρυθμιστικές εξουσίες των εθνικών αρχών** ενισχύθηκαν στη μεγάλη πλειονότητα των κρατών μελών.
- Τα περισσότερα κράτη μέλη έχουν θέσει σε εφαρμογή συγκεκριμένες δραστηριότητες για την **ενίσχυση των απαιτήσεων** για τους φορείς εκμετάλλευσης δικτύων κινητών επικοινωνιών.
- Σε όλα σχεδόν τα κράτη μέλη, με ελάχιστες εξαιρέσεις, έχουν εγκριθεί, προταθεί ή προγραμματιστεί μέτρα που αποσκοπούν στην εφαρμογή **περιορισμών με βάση το προφίλ κινδύνου των προμηθευτών**. Ως εκ τούτου, η εξάρτηση από προμηθευτές υψηλού κινδύνου αναμένεται να μειωθεί κατά τα επόμενα έτη.
- Αρκετά κράτη μέλη έχουν θεσπίσει μέτρα για τη **διαφοροποίηση**.
- Δεκαπέντε κράτη μέλη έχουν πλέον θεσπίσει **εθνικούς μηχανισμούς ελέγχου των άμεσων ξένων επενδύσεων (ΑΞΕ)**.

Ποια είναι τα επόμενα βήματα στη διαδικασία συντονισμού της ΕΕ για την κυβερνοασφάλεια δικτύων 5G;

Η Επιτροπή καλεί τα κράτη μέλη να ολοκληρώσουν την εφαρμογή των κυριότερων μέτρων της εργαλειοθήκης έως το δεύτερο τρίμηνο του 2021 και να διασφαλίσουν τον επαρκή μετριασμό των εντοπισθέντων κινδύνων, με συντονισμένο τρόπο, ιδίως για να ελαχιστοποιηθεί η έκθεση σε προμηθευτές υψηλού κινδύνου και να αποφευχθεί η εξάρτηση από τους εν λόγω προμηθευτές.

Τα συγκεκριμένα μέτρα είναι τα εξής:

- **Συνέχιση και εντατικοποίηση της ανταλλαγής πληροφοριών και βέλτιστων πρακτικών** σχετικά με συγκεκριμένα στρατηγικά και τεχνικά μέτρα, καθώς και σχετικά με επικαιροποιημένες εθνικές εκτιμήσεις κινδύνου στο πλαίσιο του άξονα εργασίας της ομάδας συνεργασίας NIS
- **Παρακολούθηση των εξελίξεων** στην τεχνολογία 5G
- Αξιοποίηση των **δυνατοτήτων ενωσιακής χρηματοδότησης**
- Καθορισμός και εφαρμογή συγκεκριμένου σχεδίου δράσης για την **ενίσχυση της εκπροσώπησης της ΕΕ σε φορείς καθορισμού προτύπων**
- Προετοιμασία **υποψήφιου συστήματος πιστοποίησης για τις βασικές συνιστώσες των δικτύων 5G και τις διαδικασίες των προμηθευτών**
- Εργασίες για την **ανθεκτικότητα των αλυσίδων εφοδιασμού**
- Επενδύσεις σε **ικανότητες έρευνας και καινοτομίας**.

4. Πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων

Τι νέο υπάρχει στη σημερινή πρόταση;

Οι υποδομές, τα δίκτυα και οι φορείς εκμετάλλευσης που παρέχουν βασικές υπηρεσίες συνδέονται όλο και περισσότερο, το οποίο σημαίνει ότι οι ελλείψεις σε μία επιχείρηση σε έναν τομέα μπορούν να προκαλέσουν διαταραχές σε πολλούς άλλους οικονομικούς τομείς σε ολόκληρη την εσωτερική αγορά.

Η πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων διευρύνει το πεδίο εφαρμογής των υφιστάμενων κανόνων της ΕΕ για τις υποδομές ζωτικής σημασίας. Καλύπτονται πλέον δέκα τομείς: ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγεία, πόσιμο νερό, λύματα, ψηφιακή υποδομή, δημόσια διοίκηση και διάστημα, ενώ οι υφιστάμενοι κανόνες της ΕΕ εφαρμόζονταν μόνο στους τομείς της ενέργειας και των μεταφορών.

Η πρόταση εισάγει επίσης νέους κανόνες για την ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων:

- Κάθε κράτος μέλος θα εγκρίνει **εθνική στρατηγική** για να διασφαλιστεί η ανθεκτικότητα των κρίσιμων οντοτήτων και θα διενεργεί τακτικές εκτιμήσεις κινδύνου.
- Οι κρίσιμες οντότητες θα υπόκεινται σε **κοινές υποχρεώσεις υποβολής εκθέσεων**, συμπεριλαμβανομένων των εκτιμήσεων κινδύνου σε επίπεδο οντότητας και της κοινοποίησης περιστατικών, και θα πρέπει να λαμβάνουν **τεχνικά και οργανωτικά μέτρα** για να διασφαλίζουν την ανθεκτικότητά τους.
- Μια ομάδα για την ανθεκτικότητα των κρίσιμων οντοτήτων, η οποία θα συγκεντρώνει τα κράτη μέλη και την Επιτροπή, θα **αξιολογεί τις εθνικές στρατηγικές** και θα διευκολύνει τη **συνεργασία και την ανταλλαγή βέλτιστων πρακτικών**.
- Ένας **μηχανισμός επιβολής** θα συμβάλει στη διασφάλιση της τήρησης των κανόνων: τα κράτη μέλη θα πρέπει να διασφαλίσουν ότι οι εθνικές αρχές θα διαθέτουν τις εξουσίες και τα μέσα για τη διενέργεια επιτόπιων επιθεωρήσεων κρίσιμων οντοτήτων. Τα κράτη μέλη θα πρέπει επίσης να θεσπίσουν ποινές σε περίπτωση μη συμμόρφωσης.
- Η Επιτροπή θα παρέχει **συμπληρωματική στήριξη στα κράτη μέλη και στις κρίσιμες οντότητες**, για παράδειγμα με την ανάπτυξη ενωσιακής επισκόπησης των διασυνοριακών και διατομεακών κινδύνων, βέλτιστων πρακτικών, μεθοδολογιών, διασυνοριακών δραστηριοτήτων κατάρτισης και ασκήσεων για τον έλεγχο της ανθεκτικότητας των κρίσιμων οντοτήτων.

Ποια είδη κινδύνων επιδιώκει να αντιμετωπίσει η πρόταση;

Η πρόταση καλύπτει όλους τους κινδύνους, δηλαδή λαμβάνει υπόψη όλους τους σχετικούς φυσικούς και ανθρωπογενείς κινδύνους, συμπεριλαμβανομένων των ατυχημάτων, των φυσικών καταστροφών, των ανταγωνιστικών απειλών, όπως τρομοκρατικές πράξεις, και των καταστάσεων έκτακτης ανάγκης στον τομέα της δημόσιας υγείας, μεταξύ των οποίων και οι πανδημίες, όπως αυτή που αντιμετωπίζει σήμερα η Ευρώπη. Η πρόταση διαφέρει από την οδηγία για τις ευρωπαϊκές υποδομές ζωτικής σημασίας, η οποία επικεντρώνεται κυρίως στην τρομοκρατία.

Τι είδους υποχρεώσεις θα επιβάλει στα κράτη μέλη;

Τα κράτη μέλη θα πρέπει να εγκρίνουν στρατηγική για τη διασφάλιση της ανθεκτικότητας των κρίσιμων οντοτήτων, να διενεργήσουν εκτίμηση κινδύνου για όλους τους κινδύνους, να ορίσουν αρμόδια αρχή/αρμόδιες αρχές και ένα εθνικό σημείο επαφής. Με βάση την εκτίμηση κινδύνου, κάθε κράτος μέλος θα πρέπει να προσδιορίσει τις κρίσιμες οντότητες σε διάφορους τομείς. Υπάρχουν επίσης διατάξεις για καλύτερη ευρωπαϊκή συνεργασία.

Τι είδους υποχρεώσεις θα επιβάλει στις οντότητες;

Εκτός από την εθνική εκτίμηση κινδύνου που θα διεξαχθεί από τις εθνικές αρχές, οι κρίσιμες οντότητες θα πρέπει να διενεργήσουν δική τους εκτίμηση κινδύνου. Αυτή η εκτίμηση σε επίπεδο οντότητας θα πρέπει να λαμβάνει υπόψη τόσο τα αποτελέσματα της εκτίμησης κινδύνου σε εθνικό επίπεδο όσο και τις τοπικές συνθήκες και ιδιαιτερότητες. Σε αυτήν τη βάση, θα πρέπει να λάβουν τεχνικά και οργανωτικά μέτρα για την ενίσχυση της ανθεκτικότητάς τους. Θα πρέπει επίσης να παρέχουν στις αρμόδιες αρχές πληροφορίες σχετικά με περιστατικά και πιθανά περιστατικά.

Περισσότερες πληροφορίες

Δελτίο Τύπου: Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων

Ενημερωτικό δελτίο σχετικά με τη νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια

Ενημερωτικό δελτίο για την πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο

κυβερνοασφάλειας σε ολόκληρη την Ένωση (αναθεωρημένη οδηγία NIS)

Ενημερωτικό δελτίο σχετικά με την κυβερνοασφάλεια: εξωτερική δράση της ΕΕ

Πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (αναθεωρημένη οδηγία NIS ή «NIS 2»)

Πρόταση οδηγίας σχετικά με την ανθεκτικότητα των κρίσιμων οντοτήτων (βλ. επίσης παράρτημα 1 της πρότασης, καθώς και την εκτίμηση επιπτώσεων και την περίληψή της)

Ευρωπαϊκή Ένωση Ασφάλειας

Εκτίμηση επιπτώσεων σχετικά με την αναθεωρημένη οδηγία NIS («NIS 2»)

Περισσότερα για την κυβερνοασφάλεια

Περισσότερα για την οδηγία NIS

QANDA/20/2392

Αρμόδιοι επικοινωνίας:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Ερωτήσεις του κοινού: Europe Direct τηλεφωνικά 00 800 67 89 10 11 ή με ηλεκτρονικό μήνυμα