Η σημαντική αύξηση στις απειλές στον κυβερνοχώρο σε ζωτικής σημασίας υπηρεσίες και υποδομές, καλούν για ενισχυμένη συνεργασία μεταξύ φορέων του ιδιωτικού και δημοσίου τομέα

Με τη μελέτη του σχετικά με τις υποδομές πληροφοριών ζωτικής σημασίας (ΥΖΣ), ο ENISA αναλύει τις τρέχουσες πρακτικές ΥΠΖΣ και τα μοντέλα διακυβέρνησης που έχουν αναπτυχθεί στα κράτη μέλη της ΕΕ. Η μελέτη αυτή συμβάλλει στην επικύρωση και στη μελλοντική εφαρμογή της Οδηγίας NIS.

Πολίτες και επιχειρήσεις εξαρτώνται από τις υποδομές πληροφοριών και επικοινωνιών για την υποστήριξη online υπηρεσιών ζωτικής σημασίας (π.χ. ενέργεια, τηλεπικοινωνίες, υγειονομική περίθαλψη). Η αύξηση των απειλών στον κυβερνοχώρο μπορεί να επηρεάσει σε μεγάλο βαθμό την παροχή υπηρεσιών και να οδηγήσει σε απώλεια χρημάτων και φήμης για επιχειρήσεις.

Τα κράτη μέλη της ΕΕ και ο ιδιωτικός τομέας ομοίως θα πρέπει να συνεργαστούν μεταξύ τους, αν επιθυμούν σήμερα να αντιμετωπίσουν αποτελεσματικά τις απειλές αυτές. Ωστόσο, μόνο οι μισές από τις εξεταζόμενες χώρες έχουν θεσπίσει τέτοιου είδους μοντέλα συνεργασίας δημόσιου-ιδιωτικού τομέα, ομάδες εργασίας και φόρουμ επικοινωνίας.

Καθώς ορισμένοι τομείς, όπως ο χρηματοπιστωτικός, οι τηλεπικοινωνίες και η ενέργεια έχουν πιο αυστηρούς κανόνες σε σύγκριση με άλλους, οι απαιτήσεις ασφαλείας διαφέρουν σημαντικά σε όλους τους τομείς και σε διαφορετικούς τύπους φορέων ΥΖΣ. Μόνο ένας μικρός αριθμός χωρών έχει εφαρμόσει τις υποχρεωτικές απαιτήσεις ασφαλείας σε όλους τους τομείς.

Η μελέτη επισημαίνει πως ορισμένες χώρες, ειδικά σε αυτές με μια πιο αποκεντρωμένη προσέγγιση ΥΠΖΣ, αναθέτουν την εθνική αξιολόγηση κινδύνων τους σε Αρχές που σχετίζονται με τον τομέα ή σε φορείς ΥΖΣ. Κάποιες χώρες πιστεύουν ότι η πίεση της αγοράς θα δώσει στους φορείς ΥΖΣ επαρκή κίνητρα για να επενδύσουν σε πρόσθετα μέτρα ασφαλείας. Ωστόσο, σχεδόν κανένα από τα εξεταζόμενα κράτη μέλη δεν έχει εφαρμόσει κίνητρα για να επενδύσει σε μέτρα ασφαλείας που σχετίζονται με τις ΥΠΖΣ για τους φορείς ΥΖΣ.

Έπειτα από τα επικυρωμένα αποτελέσματα της μελέτης, ο ENISA προτείνει στα κράτη μέλη και στην Ευρωπαϊκή Επιτροπή να:

- διενεργήσουν σχολαστική εθνική αξιολόγηση κινδύνων
- θεσπίσουν συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων
- ορίσουν τις βασικές απαιτήσεις ασφάλειας για υποστήριξη της ανάπτυξης ΥΠΖΣ στα ΚΜ
- εφαρμόσουν κίνητρα που θα μπορούσαν να παροτρύνουν τους φορείς ΥΖΣ να επενδύσουν περισσότερο σε μέτρα ασφαλείας

Ο Udo Helmbrecht, Εκτελεστικός Διευθυντής του ENISA, δήλωσε: *«Οι προκύπτουσες απειλές σε υποδομές πληροφοριών ζωτικής σημασίας αποτελούν σαφή και υφιστάμενο κίνδυνο. Κίνδυνος ο οποίος μπορεί να μετριαστεί μόνο με συντονισμένες προσπάθειες. Ο ENISA συνεργάζεται τόσο με δημόσιους όσο και με ιδιωτικούς φορείς για να βεβαιωθεί ότι οι ΥΠΖΣ αποτελούν προτεραιότητα σε επίπεδο ΕΕ».*

Ο ENISA παρέχει συμβουλές, συστάσεις και βοήθεια στα κράτη μέλη της ΕΕ αναφορικά με την εφαρμογή της σχετικής νομοθεσίας της ΕΕ. Ο οργανισμός εμπλέκει φορείς και τη βιομηχανία στην ανταλλαγή ορθών πρακτικών, πληροφοριών και ιδεών με στόχο τη βελτίωση της προστασίας των ΥΠΖΣ στην Ευρώπη.

Εν όψει της επικείμενης Οδηγίας NIS και με βάση τα ευρήματα της έκθεσης αυτής, ο ENISA θα συνεχίσει να εργάζεται πάνω σε θέματα ΥΠΖΣ με τη συμμετοχή δημόσιων και ιδιωτικών φορέων, ώστε να καθορίσουν τις βασικές απαιτήσεις ασφαλείας και μια εναρμονισμένη προσέγγιση για την αναφορά συμβάντων.

Πλήρης έκθεση: Περισσότερα ευρήματα και πρόσθετες πληροφορίες σχετικά με τη μελέτη
Για τεχνικές πληροφορίες: Anna Sarri, Υπεύθυνη της NIS, Anna.sarri@enisa.europa.eu
Για συνεντεύξεις και ερωτήματα από τον Τύπο επικοινωνήστε με press@enisa.europa.eu, Τηλ: +30 2814 409576