

Ο Εκτελεστικός Διευθυντής του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) παραθέτει ομιλία σε συνδιάσκεψη του ΕΚ με θέμα μια ισορροπημένη προσέγγιση αναφορικά με την ιδιωτικότητα στο διαδίκτυο, σε συνδυασμό με έναν αξιόπιστο τομέα ΤΠΕ στην ΕΕ

«Η πρόκληση για τους υπεύθυνους χάραξης πολιτικών είναι να επιτευχθεί ισορροπημένη προσέγγιση αναφορικά με την ιδιωτικότητα, με τις ελάχιστες δυνατές αρνητικές επιπτώσεις στα συμφέροντα των πολιτών και τις δραστηριότητες του κλάδου», δήλωσε ο Udo Helmreich, Εκτελεστικός Διευθυντής του ENISA, κατά την υψηλού επιπέδου συνδιάσκεψη του Ευρωπαϊκού Κοινοβουλίου στις Βρυξέλλες. Η συνδιάσκεψη διοργανώθηκε από κοινού από την Επιτροπή Πολιτικών Ελευθεριών (LIBE) και τη Λουξεμβουργιανή Προεδρία του Συμβουλίου της ΕΕ, με συμπροεδρία των επιτροπών IMCO και ITRE, και εξετάζει την προστασία της ιδιωτικότητας στο διαδίκτυο, ενισχύοντας την ασφάλεια της ΤΠ αλλά και τις δυνατότητες ΤΠ της ΕΕ.

Ο ENISA χαιρέτισε τους τομείς πολιτικής που συζητήθηκαν ξεχωριστά με στόχο να παροτρύνει την υιοθέτηση τόνωσης της έγκρισης τεχνολογιών για καλύτερη προστασία της ιδιωτικής ζωής (PET), την αντιμετώπιση τρωτοτήτων σε λογισμικά και υλισμικά και τις υποδομές του διαδικτύου, καθώς επίσης ανάπτυξη του δυναμικού της ΕΕ για ένα ισχυρό και δυναμικό κλάδο ΤΠ. Ο ENISA ελπίζει να υπάρξει ενθαρρυντικό αποτέλεσμα από τη συνδιάσκεψη κατά την πολιτική συζήτηση σχετικά με αυτές τις στενά συνδεδεμένες πολιτικές.

Οι PET, η τυποποίηση και η πιστοποίηση αποτελούν τη βάση για τον κλάδο της ΤΠ

Η χρήση των PET ως 'προστασία της ιδιωτικής ζωής' ήδη από τον σχεδιασμό' αποτελούν μέρος της λειτουργικότητας της ΤΠ, προσφέροντας προστασία της ιδιωτικότητας συμβατή με και βασισμένη σε πρότυπα χαρακτηριστικά ασφαλείας, ενώ ενθαρρύνεται η εφαρμογή τους από προεπιλογή. Επιπρόσθετα, οι κατευθυντήριες γραμμές της ΕΕ που καταπιάνονται με την ανάπτυξη ασφαλών λογισμικών και υλισμικών, όπως η τυποποίηση και η πιστοποίηση, τα οποία αναπτύσσει και ο ENISA, μπορούν να προωθηθούν και εφαρμοστούν στο σύνολο της ΕΕ, ως μέσο για την αντιμετώπιση τρωτοτήτων.

Η θέσπιση του Διαδικτύου των Αντικειμένων (IoT) αποτελεί παράδειγμα που καταδεικνύει την αυξημένη σημασία τους, καθώς συνεπάγεται προκλήσεις ασφαλείας που μπορούν να μετριάσουν εν μέρει από άποψη ανθεκτικότητας του δικτύου. Ωστόσο, η αλληλεπίδραση των IoT με στοιχεία λογισμικού και υλισμικού εισάγει περισσότερους κινδύνους και απειλές. Από αυτή την άποψη, ορισμένα στοιχεία της αρχιτεκτονικής διαδικτύου διαδραματίζουν καίριο ρόλο. Συνεπώς, είναι σημαντικό να υπάρξει θέσπιση ανταλλαγής πληροφοριών σχετικά με περιστατικά και τρωτότητες, καθώς επίσης διάλογος μεταξύ των φορέων που μπορούν να βοηθήσουν με στόχο μια κοινή προσέγγιση για την ασφάλεια.

Αναφορικά με την αντιμετώπιση της κρισιμότητας των υποδομών ΤΠ της ΕΕ, τα κράτη μέλη έχουν αναπτύξει ειδικά μέτρα για την προστασία τους. Το **νέο κείμενο που συμφωνήθηκε** στην οδηγία NIS αποτελεί θετικό βήμα για μια πιο εναρμονισμένη προσέγγιση και συνεργασία μεταξύ όλων των φορέων και κλάδων, έχοντας ως αντικείμενο την ασφάλεια των ψηφιακών υποδομών (είτε ενέργειας, υγείας, μεταφορών ή οικονομικών), προκειμένου να εξασφαλιστεί υψηλό επίπεδο ασφαλείας για καίρια συστήματα, υποδομές και πολίτες. Ο ENISA έχει εκτενή εμπειρία στους τομείς αυτούς. Με την εμπειρία του αναπτύχθηκαν μηχανισμοί ορθής συνεργασίας (μέσω CSIRT και ασκήσεων της σειράς Cyber Europe) επιτρέποντας στις αρμόδιες Αρχές μαζί με

τον ιδιωτικό τομέα να αποκριθούν σε περιστατικά (άρθρο 13α, TSP).¹ «Προσβλέπουμε σε περαιτέρω ενίσχυση και ενδυνάμωση της συνεργασίας μας προς αυτή την κατεύθυνση», δήλωσε ο **Helmbrecht**.

Ο ENISA επισημαίνει την προστιθέμενη αξία της αγοράς ασφάλειας στον κυβερνοχώρο

Κατά τη συζήτηση επισημάνθηκαν οι επιτρεπτές τιμές που προκύπτουν από την ασφάλεια στον κυβερνοχώρο, οι οποίες δύνανται να ανέλθουν σε 640 δισ.² ευρώ για την οικονομία της ΕΕ. Η αγορά της ΕΕ για ασφάλεια στον κυβερνοχώρο είναι υπανάπτυκτη, με εκτιμώμενη αξία 20 δισ. ευρώ και ανάπτυξη 6% του CAGR (Σύνθετος Ρυθμός Ετήσιας Ανάπτυξης)³. Το σημαντικό για την ΕΕ είναι να θεσπίσει εμπιστοσύνη μεταξύ πολιτών και κλάδου σε σχέση με τον κυβερνοχώρο, ώστε να δημιουργηθεί ένας ανταγωνιστικός τομέας ΤΠΕ με βάση την ΕΕ, ενισχύοντας περαιτέρω τη θέση της ΕΕ.

Για περισσότερες πληροφορίες επί του θέματος καθώς και ερωτήματα από τον Τύπο, επικοινωνήστε με τα press@enisa.europa.eu, Τηλ. +30 2814 409576

Για περισσότερες πληροφορίες σχετικά με τη συνεδρίαση του ΕΚ, επισκεφθείτε:

<http://www.europarl.europa.eu/committees/en/libe/events.html?id=20151208CHE00191>

<http://www.stoa.europarl.europa.eu/stoa/cms/home/events/workshops/privacy>

¹TSP (Πάροχοι Υπηρεσιών Εμπιστευσης). Ο ENISA προτείνει ένα **νέο σύστημα υποβολής αναφορών για τους TSP** Άρθρο 13α: Το άρθρο 13α, της Οδηγίας 2009/140 του ΕΚ, αποτελεί μέρος του Πακέτου Τηλεπικοινωνιών και αποσκοπεί στο να εξασφαλίσει την ασφάλεια και ακεραιότητα των δικτύων ηλεκτρονικών επικοινωνιών και υπηρεσιών (τηλεπικοινωνιών). Στον τομέα αυτό, ο **ENISA** έχει την ευθύνη να συλλέγει περιστατικά και ενέργειες που λαμβάνουν χώρα στους τομείς τηλεπικοινωνιών των κρατών μελών, καθώς επίσης να συμβάλλει στην «εναρμόνιση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας, παρέχοντας εξειδικευμένες συμβουλές» και «προωθώντας την ανταλλαγή ορθών πρακτικών».

² Κίνδυνος και Ευθύνη σε έναν Κόσμο με Εξάρτηση από το Διαδίκτυο - Παγκόσμιο Οικονομικό Φόρουμ

³ Μέγεθος αγοράς ασφάλειας στον κυβερνοχώρο στην Ευρώπη – Gartner 2014