30/01/2014

EPR08/2014

www.enisa.europa.eu

Ενέργεια: η ασφάλεια στον κυβερνοχώρο είναι καθοριστική για την προστασία από τις απειλές κατά των έξυπνων ενεργειακών δικτύων, τα οποία παίζουν βασικό ρόλο στη διαθεσιμότητα ενέργειας, υποστηρίζει σε νέα έκθεση ο Οργανισμός της ΕΕ για την ασφάλεια στον κυβερνοχώρο.

Ο Οργανισμός ENISA της ΕΕ για την ασφάλεια στον κυβερνοχώρο καταδεικνύει ότι η εκτίμηση των απειλών κατά των έξυπνων ενεργειακών δικτύων είναι καθοριστική για την προστασία τους, και ως εκ τούτου αποτελεί βασικό στοιχείο της διασφάλισης διαθέσιμης ενέργειας.

Τα έξυπνα ενεργειακά δίκτυα είναι περίπλοκα «συστήματα συστημάτων», που αποθηκεύουν, μεταφέρουν και διαχειρίζονται την ενέργεια από την παραγωγή έως τους καταναλωτές. Ένα έξυπνο ενεργειακό δίκτυο αποτελεί εκ των πραγμάτων υποδομή ζωτικής σημασίας, καθώς η ενέργεια είναι καθοριστική για την κοινωνία και για την καλή λειτουργία της οικονομίας. Συνδυάζοντας υποδομές ενέργειας και πληροφοριών, τα έξυπνα ενεργειακά δίκτυα συνιστούν υποδομές ζωτικής σημασίας και θα πρέπει να λειτουργούν με ασφάλεια, κάνοντας σεβαστή την ιδιωτική ζωή των τελικών χρηστών.

Ο Καθηγητής Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, σχολίασε: «*Η κατανόηση του τοπίου των απειλών στον κυβερνοχώρο είναι απαραίτητη για να προσδιοριστεί ποια προστατευτικά μέτρα είναι αναγκαία για τα έξυπνα ενεργειακά δίκτυα. Αυτή η έκθεση αποτελεί απάντηση στο πιεστικό ερώτημα των παρόχων και φορέων ενέργειας: παρέχει τα εργαλεία για να εκτιμηθεί η έκθεση των πόρων των έξυπνων ενεργειακών δικτύων στον κίνδυνο. Στην ασφάλεια στον κυβερνοχώρο χρειαζόμαστε κοινές προσπάθειες και κοινό συντονισμό για να μειώσουμε τις επιπτώσεις*».

Αυτή η έκθεση παρουσιάζει ένα τοπίο των απειλών που πλήττουν τα συστατικά μέρη των έξυπνων ηλεκτρικών δικτύων. Κάνει μια γενική εκτίμηση των διαθέσιμων προσεγγίσεων της ασφάλειας και της προστασίας στον κυβερνοχώρο, καθώς και των ορθών πρακτικών στον τομέα αυτό. Η μελέτη απαριθμεί επίσης τις εσωτερικές απειλές που πλήττουν τους πόρους των έξυπνων ενεργειακών δικτύων που σχετίζονται με την τεχνολογία των πληροφοριών, συμπεριλαμβανομένων διαφόρων απειλών που απορρέουν από σφάλματα και από επιθέσεις προσώπων που κατέχουν εμπιστευτικές θέσεις.

Βασικά συμπεράσματα: Μερικά από τα βασικά συμπεράσματα που εντοπίστηκαν είναι:

- *Λάβετε υπόψη τις εξωτερικές και εσωτερικές απειλές*: στην ασφάλεια στον κυβερνοχώρο, οι εξωτερικές απειλές του κυβερνοχώρου αποτελούν την κύρια πηγή εξωτερικής έκθεσης. Αυτό το περιβάλλον απειλών στον κυβερνοχώρο προέρχεται από παράγοντες απειλής που εκμεταλλεύονται τις απειλές στον κυβερνοχώρο και εξαπολύουν επιθέσεις στον κυβερνοχώρο.
- *Αποσυνθέστε και ταξινομήστε τα στοιχεία των έξυπνων ενεργειακών δικτύων που εκτίθενται σε απειλές*: από τους ηλεκτρικούς πόρους, όπως καλώδια, διακόπτες, δρομολογητές, αισθητήρες και πληροφορίες, μέχρι το λογισμικό, όπως λειτουργικά συστήματα, υπηρεσίες, υλικό εξοπλισμό, υποδομή και τα άτομα που χειρίζονται τα συστήματα.
- *Χρησιμοποιήστε τις διαθέσιμες γνώσεις*: ξαναχρησιμοποιήστε τις υπάρχουσες ορθές πρακτικές αφού προσδιορίσετε το επίπεδο της επιθυμητής προστασίας.
- *Απαριθμήστε τις **συγκεκριμένες απειλές στον κυβερνοχώρο κατά των έξυπνων ενεργειακών δικτύων**, για παράδειγμα:*
    - *Λαθρακρόαση/υποκλοπή/σφετερισμός: π.χ. διαρροή πληροφοριών, ηλεκτρομαγνητική υποκλοπή/υποκλοπή ραδιοσυχνοτήτων, επιθέσεις ανίχνευσης, βλάβες συσκευών και συστημάτων, επιθέσεις και φυσικές επιθέσεις,*

      *και τους **παράγοντες απειλής,** όπως εταιρείες, εγκληματίες του κυβερνοχώρου, υπαλλήλους, χακτιβιστές, εθνικά κράτη, φυσικές καταστροφές, τρομοκράτες, το νέο στοιχείο των μαχητών στον κυβερνοχώρο.*
- *Εκτιμήστε τις ευπάθειες και τους κινδύνους στα έξυπνα ενεργειακά δίκτυα.*
- *Εκτιμήσεις που πρέπει να γίνουν από τους ιδιοκτήτες των πόρων*: Τέλος, ο Οργανισμός συμπεραίνει ότι η εκτίμηση της έκθεσης ενός έξυπνου ενεργειακού δικτύου στις απειλές και τους κινδύνους μπορεί να γίνει μόνο από τον ιδιοκτήτη του πόρου, ο οποίος κατέχει πλήρως την περιπλοκότητα και τις αλληλεξαρτήσεις των σχετιζόμενων υποδομών έξυπνων ενεργειακών δικτύων.

Για την πλήρη έκθεση

Γενικές πληροφορίες: Εκθέσεις του ENISA για τα Έξυπνα ενεργειακά δίκτυα (Δεκέμβριος 2012), 10 συστάσεις (Ιούλιος 2012)
Η Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο, η πρόταση για μια Οδηγία της ΕΕ για την ασφάλεια στον κυβερνοχώρο

Δελτίο Τύπου

30/01/2014

EPR08/2014

www.enisa.europa.eu

Για συνεντεύξεις: Ulf Bergström, Εκπρόσωπος Τύπου, ulf.bergstrom@enisa.europa.eu, κινητό: +30 6948 460 143, ή Δρ. Λούης Μαρίνος, Εμπειρογνώμων του ENISA, resilience@enisa.europa.eu

Μετάφραση. Η έκδοση στην αγγλική γλώσσα είναι η μόνη έγκυρη.

http://www.enisa.europa.eu/media/enisa-in-greek/

www.enisa.europa.eu