09/02/2015

EPR06/2015

www.enisa.europa.eu

Είναι τα έξυπνα σπίτια ευφυή από άποψη ασφάλειας στον κυβερνοχώρο;

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δημοσίευσε σήμερα την έκθεση με τίτλο Τοπίο απειλών και οδηγός ορθής πρακτικής για το έξυπνο σπίτι και τα μέσα σύγκλισης, συμβάλλοντας έτσι στην προσπάθεια επίτευξης των στόχων που διατυπώνονται στη στρατηγική ασφάλειας στον κυβερνοχώρο για την ΕΕ. Στόχος της μελέτης είναι να εντοπίσει αφενός τους κινδύνους και τις προκλήσεις της ασφάλειας και αφετέρου τα αντίμετρα που απαιτούνται για τις αναδυόμενες τεχνολογίες στα έξυπνα σπίτια, παρέχοντας συγκεκριμένη και εστιασμένη προσέγγιση, με μια επισκόπηση της τρέχουσας κατάστασης της ασφάλειας στον κυβερνοχώρο σε αυτόν τον αναδυόμενο τομέα.

Για τη σύνταξη αυτής της έκθεσης δημιουργήθηκε μια ανεπίσημη ομάδα εμπειρογνωμόνων, προκειμένου να συλλεχθούν στοιχεία σε διάφορα στάδια του έργου. Επιπλέον, η μελέτη λαμβάνει υπόψη υπάρχουσες αξιολογήσεις και δημοσίως διαθέσιμες πηγές πληροφοριών, παρέχοντας ένα θεματικό Τοπίο απειλών στον τομέα των έξυπνων σπιτιών.

Στο πλαίσιο του πεδίου εφαρμογής της μελέτης έχουν εντοπιστεί παράγοντες απειλής που αποκαλύπτουν αρκετές πηγές τρωτότητας. Οι εγκληματίες του κυβερνοχώρου κατατάσσονται ως η μεγαλύτερη και εχθρικότερη κατηγορία απειλών, ενώ η ενδεχόμενη κατάχρηση των έξυπνων σπιτιών θα πρέπει να θεωρηθεί ιδιαίτερα πιθανή δεδομένου του αυξανόμενου αριθμού έξυπνων συσκευών και σπιτιών, αλλά και ιδιαίτερα των μέσων σύγκλισης. Επιπλέον, αρκετοί οικονομικοί παράγοντες δημιουργούν τρωτότητες ασφάλειας, ενώ οι σχεδιαστικές επιλογές ανταγωνίζονται το κόστος και την πρακτικότητα.

Πολλοί από τους κινδύνους είναι κοινωνικοτεχνικής φύσης λόγω του βάθους και της ποικιλίας των προσωπικών πληροφοριών που μπορούν να καταγραφούν και να αποτελέσουν αντικείμενο επεξεργασίας, ενώ οδηγούν στην παραγωγή δεδομένων για προηγουμένως μη καταγεγραμμένες δραστηριότητες, συνδέοντας στενά τους ανθρώπους και το περιβάλλον τους. Επιπλέον, τα συμφέροντα των διαφόρων ιδιοκτητών περιουσιακών στοιχείων στο έξυπνο σπίτι δεν είναι κατ' ανάγκη ευθυγραμμισμένα – μπορεί μάλιστα και να συγκρούονται –, γεγονός που δημιουργεί ένα περίπλοκο περιβάλλον για δραστηριότητες ασφάλειας.

Από την άλλη, τα μέσα σύγκλισης και η τηλεόραση εγείρουν ζητήματα ασφάλειας από άποψη συνδεσιμότητας, ενσωματωμένης λειτουργικότητας, αδιαφανών συστημάτων και ασυμβατότητας με τις παραδοσιακές προσεγγίσεις ασφάλειας των πληροφοριών, καθώς και ζητήματα ιδιωτικότητας, πρόσβασης και δικαιωμάτων πνευματικής ιδιοκτησίας. Οι συσκευές μέσων σύγκλισης είναι πιθανόν να είναι κάποιες από τις πρώτες καταναλωτικές συσκευές έξυπνου σπιτιού που θα εισαχθούν σε πολλά σπίτια, και ως εκ τούτου, θα είναι το αρχικό πεδίο δράσης πολλών από τα εντοπισμένα ζητήματα ασφάλειας έξυπνου σπιτιού.

Λόγω των πολλαπλών τρόπων σχεδιασμού δεν δημιουργούνται όλα τα έξυπνα σπίτια ισότιμα. Αυτοί οι τρόποι μπορεί να οδηγήσουν στις δικές τους ιδιαιτερότητες ασφάλειας και ιδιωτικότητας, με κοινά ζητήματα και τρωτότητες. Όπως ακριβώς και σε πολλούς άλλους τομείς των ΤΠΕ, η εφαρμογή βασικής ασφάλειας των πληροφοριών μπορεί να αυξήσει σημαντικά τη γενική ασφάλεια στον τομέα του έξυπνου σπιτιού.

Οι ορθές πρακτικές στον τομέα αυτό περιλαμβάνουν το σχεδιασμό του έξυπνου σπιτιού ως συστήματος, την προσεκτική εξέταση της ασφάλειας των σχεδίων έξυπνου σπιτιού που βασίζονται στο υπολογιστικό νέφος, ένα πλαίσιο απομόνωσης των εφαρμογών (όπως σχεδιάζεται για τα έξυπνα αυτοκίνητα) και διαχωρισμό του κρίσιμου λογισμικού από μη κρίσιμες εφαρμογές, αλλά και μέτρα ασφάλειας δικτύου και επικοινωνιών. Παρόμοιες προσεγγίσεις με αυτές που αναφέρθηκαν για τα έξυπνα δίκτυα μπορεί να αποδειχθούν εφαρμόσιμες και στο πλαίσιο των έξυπνων σπιτιών.

Ο εκτελεστικός διευθυντής Udo Helmbrecht δήλωσε: *«Το έξυπνο σπίτι είναι ένα σημείο έντονης επαφής ανάμεσα στη δικτυωμένη τεχνολογία των πληροφοριών και στον φυσικό χώρο, συνεπώς συνδυάζει κινδύνους ασφάλειας τόσο από το εικονικό όσο και από το φυσικό περιβάλλον. Ο εντοπισμός των απειλών στον κυβερνοχώρο είναι κρίσιμος για την προστασία του έξυπνου σπιτιού και ως εκ τούτου αποτελεί βασικό στοιχείο για τη διασφάλιση της επιτυχούς ανάπτυξής του».*

Για την πλήρη έκθεση: Τοπίο απειλών για το έξυπνο σπίτι και τη σύγκλιση των μέσων

Για συνεντεύξεις και επικοινωνία με τους συγγραφείς χρησιμοποιήστε τη διεύθυνση resilience@enisa.europa.eu, **για ερωτήσεις των ΜΜΕ** press@enisa.europa.eu

Σημειώσεις προς τους συντάκτες:

Ετήσιες εκθέσεις του ENISA Τοπίο απειλών **2014**,**2013**,**2012**

ENISA – Θεματικά τοπία για τις απειλές:

Τοπίο απειλών και οδηγός ορθής πρακτικής για την υποδομή του διαδικτύου (2014)

Τοπίο απειλών και οδηγός ορθής πρακτικής για τα έξυπνα δίκτυα (2013)