19 Ιουνίου 2022

Κυβερνοασφάλεια: Τρωτά σημεία σε routers – Πόσα ανακαλύφθηκαν το 2021 – Οικονομικός Ταχυδρόμος

/ Επιστήμες, Τέχνες & Πολιτισμός

Τα routers είναι απαραίτητα για συνδέσεις Wi-Fi, καθώς εκατομμύρια νέες συσκευές εγκαθίστανται καθημερινά σε σπίτια και χώρους εργασίας

OT.gr Newsroom

Σύμφωνα με ανάλυση που πραγματοποιήθηκε από την Kaspersky, πάνω από 500 ευπάθειες ανακαλύφθηκαν σε routers το 2021, συμπεριλαμβανομένων 87 κρίσιμων.

Οι απειλές που προέρχονται από ευάλωτα routers επηρεάζουν τόσο τα νοικοκυριά όσο και τους οργανισμούς, καθώς δεν περιορίζονται μόνο σε παραβιάσεις email και ενδέχεται να επηρεάσουν ακόμα και τη φυσική ασφάλεια του σπιτιού. Παρόλα αυτά, οι άνθρωποι σπάνια σκέφτονται την ασφάλεια των συσκευών τους.

Σύμφωνα με την έρευνα, το 73% των χρηστών δεν έχει σκεφτεί ποτέ να αναβαθμίσει ή να ασφαλίσει το router τους, καθιστώντας το μία από τις μεγαλύτερες απειλές που επηρεάζουν το Internet of Things σήμερα. Εδώ, οι ειδικοί της Kaspersky εξηγούν ποιες απειλές μπορεί να αποτελούν τα τρωτά σημεία του router και πώς οι χρήστες μπορούν να προστατευτούν.

Ο ρόλος του router

Το router είναι ο κόμβος ενός ολόκληρου οικιακού δικτύου, μέσω του οποίου όλα τα στοιχεία ενός «έξυπνου» σπιτιού έχουν πρόσβαση στο διαδίκτυο και ανταλλάσσουν δεδομένα. Μολύνοντας το router, οι εισβολείς αποκτούν πρόσβαση στο δίκτυο μέσω του οποίου μεταδίδονται τα πακέτα δεδομένων. Χρησιμοποιώντας αυτό, μπορούν να εγκαταστήσουν κακόβουλο λογισμικό σε συνδεδεμένους υπολογιστές για να κλέψουν ευαίσθητα δεδομένα, ιδιωτικές φωτογραφίες ή επαγγελματικά αρχεία – πιθανώς προκαλώντας ανεπανόρθωτη ζημιά στο θύμα. Μέσω του μολυσμένου router, ο εισβολέας μπορεί επίσης να ανακατευθύνει τους χρήστες σε σελίδες phishing που «μεταμφιέζονται» ως συχνά χρησιμοποιούμενα webmail ή διαδικτυακές τραπεζικές υπηρεσίες. Οποιαδήποτε δεδομένα εισάγουν σε αυτές τις σελίδες, είτε πρόκειται για τη σύνδεση και τον κωδικό πρόσβασής τους από το email ή τα στοιχεία τραπεζικής κάρτας, θα πέσουν αμέσως στα χέρια των απατεώνων.

Τα τρωτά σημεία

Από το 2010, ο αριθμός των τρωτών σημείων που εντοπίστηκαν στα routers αυξάνεται σταθερά. Το 2020, ο αριθμός των ευπαθειών που ανακαλύφθηκαν αυξήθηκε σε 603, περίπου 3 φορές περισσότερες από το προηγούμενο έτος. Το 2021, ο αριθμός των ευπαθειών που ανακαλύφθηκαν παρέμεινε σχεδόν τόσο υψηλός – 506. Από όλες τις ευπάθειες που ανακαλύφθηκαν το 2021, οι 87 ήταν κρίσιμες. Τα κρίσιμα τρωτά σημεία είναι οι πιο απροστάτευτες «τρύπες» μέσω των οποίων ένας εισβολέας μπορεί να διεισδύσει σε ένα οικιακό ή εταιρικό δίκτυο. Τέτοια τρωτά σημεία μπορεί να επιτρέψουν στον εισβολέα να παρακάμψει τον έλεγχο ταυτότητας, να στείλει απομακρυσμένες εντολές σε ένα router ή ακόμα και να το θέσει εκτός λειτουργίας. Με αυτόν τον τρόπο, οι χειριστές μπορούν να κλέψουν δεδομένα ή αρχεία που μεταδίδονται μέσω ενός «μολυσμένου» δικτύου, είτε πρόκειται για προσωπικές φωτογραφίες, ιδιωτικές πληροφορίες ή ακόμα και για επαγγελματικές συμβάσεις που αποστέλλονται σε email.

Επισφαλείς συσκευές

Αν και οι ερευνητές τώρα αυξάνουν την ευαισθητοποίηση σχετικά με πολλές περισσότερες ευπάθειες που βρέθηκαν σε σύγκριση με το παρελθόν, τα routers παραμένουν μία από τις πιο επισφαλείς συσκευές. Ένας από τους λόγους για αυτό είναι ότι δεν βιάζονται όλοι οι πωλητές να εξαλείψουν τους κινδύνους. Σχεδόν το ένα τρίτο των κρίσιμων τρωτών σημείων που ανακαλύφθηκαν το 2021 παραμένει χωρίς καμία απάντηση από τους προμηθευτές: δεν έχει εκδοθεί καμία ενημέρωση

κώδικα ή σχολιασμός με συμβουλές από αυτούς. Ακόμα ένα 26% τέτοιων τρωτών σημείων έλαβε μόνο ένα σχόλιο από την εταιρεία, το οποίο, τις περισσότερες φορές, περιλαμβάνει συστάσεις για επικοινωνία με την τεχνική υποστήριξη.

Κατανόηση της απειλής

Παράλληλα με την αυξημένη δραστηριότητα των επιτιθέμενων, οι καταναλωτές και οι μικρές επιχειρήσεις δεν έχουν την τεχνογνωσία ή τους πόρους για να εντοπίσουν ή να κατανοήσουν μια απειλή πριν να είναι πολύ αργά. Για παράδειγμα, όπως αναφέρθηκε, το 73% των χρηστών δεν έχει σκεφτεί ποτέ να αναβαθμίσει ή να ασφαλίσει το router τους, καθιστώντας το μια από τις μεγαλύτερες απειλές που επηρεάζει το «Διαδίκτυο των πραγμάτων» σήμερα. Αυτό είναι ιδιαίτερα επικίνδυνο όταν τα routers χρησιμοποιούνται σε ευαίσθητα περιβάλλοντα, όπως νοσοκομεία ή κυβερνητικά κτίρια, όπου μια διαρροή δεδομένων θα μπορούσε να έχει δυνητικά σοβαρό αντίκτυπο.

Πώς να προστασταεύσετε το router σας

Η αγορά έξυπνων συσκευών από δεύτερο χέρι είναι μια μη ασφαλής πρακτική. Το υλικολογισμικό τους θα μπορούσε να έχει τροποποιηθεί από προηγούμενους κατόχους για να δώσει σε έναν απομακρυσμένο εισβολέα τον πλήρη έλεγχο του «έξυπνου» σπιτιού σας.
Μην ξεχάσετε να αλλάξετε τον προεπιλεγμένο κωδικό πρόσβασης. Προτιμήστε έναν σύνθετο και αλλάξτε τον τακτικά.

Μην κοινοποιείτε σειριακούς αριθμούς, διευθύνσεις IP ή άλλες ευαίσθητες πληροφορίες σχετικά με τις «έξυπνες» συσκευές σας στα κοινωνικά δίκτυα.

Χρησιμοποιήστε κρυπτογράφηση WPA2 – είναι η πιο ασφαλής για μεταφορά δεδομένων.

Απενεργοποιήστε την απομακρυσμένη πρόσβαση στις ρυθμίσεις του router. Εάν εξακολουθεί να απαιτείται απομακρυσμένη πρόσβαση, θα πρέπει να την απενεργοποιήσετε όταν δεν χρησιμοποιείται.

Για περισσότερη ασφάλεια, μπορείτε να επιλέξετε μια στατική διεύθυνση IP και να απενεργοποιήσετε το DHCP, καθώς και να προστατέψετε το Wi-Fi με ένα φίλτρο MAC. Αυτές οι ενέργειες οδηγούν στο να χρειαστεί να διαμορφώσετε με μη αυτόματο τρόπο τη σύνδεση διαφόρων πρόσθετων συσκευών στο router, έτσι ώστε η διαδικασία να γίνεται πιο μακροχρόνια και πιο περίπλοκη. Ωστόσο, θα είναι πολύ πιο δύσκολο για έναν εισβολέα να διεισδύσει στο τοπικό δίκτυο. Να είστε ενήμεροι και να ελέγχετε πάντα τις πιο πρόσφατες πληροφορίες σχετικά με τις ευπάθειες

του router που ανακαλύφθηκαν.

Έχοντας αποφασίσει για την αγορά μιας συγκεκριμένης εφαρμογής ή συσκευής, φροντίστε να παραμείνετε ενήμεροι σχετικά με τις ενημερώσεις και τον εντοπισμό τρωτών σημείων.

Εγκαταστήστε έγκαιρα όλες τις ενημερώσεις που κυκλοφορούν από τους προγραμματιστές.

Εξετάστε το ενδεχόμενο να εγκαταστήσετε μια ειδική λύση ασφαλείας που μπορεί να βοηθήσει στην προστασία του οικιακού σας δικτύου και όλων των συνδεδεμένων συσκευών.

Πηγή: ot.gr