الخليج

اقتصاد, تقنية وسيارات

13 يونيو 2022 13:46 مساء

توصيات من «كاسبرسكي» لحماية «الراوتر» من الهجمات 8

دبي: «الخليج»

تُعدّ أجهزة التوجيه الشبكي (الراوتر) ضرورية لاتصالات الشبكات اللاسلكية (واي فاي)، وتُضاف ملايين أجهزة الراوتر الجديدة يومياً في المنازل وأماكن العمل حول العالم. ووفقاً لدراسة تحليلية أجرتها كاسبرسكي، فقد اكتشفت أكثر من 500 ثغرة أمنية في أجهزة الراوتر في عام 2021، بينها 87 ثغرة خطرة. وتؤثر التهديدات التي تنطوي عليها هذه الأجهزة ذات الثغرات الأمنية في المنازل والمؤسسات، وتتجاوز أخطارها مسألة اختراق البريد الإلكتروني لتصل إلى الأمن المادي للمنازل. وعلى الرغم من ذلك، من النادر أن يحسب المستخدمون حساباً لأمن أجهزتهم؛ إذ لم يفكر 73% من المستخدمين مطلقاً في ترقية جهاز الراوتر أو تأمينه، وفقاً للدراسة، ما يجعله أحد أكبر التهديدات التي تواجهها أجهزة إنترنت الأشياء اليوم.

ويُعدّ الراوتر محور الشبكة المنزلية؛ إذ يمكن من خلاله وصول جميع أجهزة المنزل الذكية إلى الإنترنت وتبادل البيانات، وبالتالي فإن إصابته قد تمكّن مجرمي الإنترنت من الوصول إلى الشبكة وتثبيت برمجيات خبيثة على أجهزة الحاسوب والهواتف المتصلة بها لسرقة البيانات الحساسة والصور وملفات العمل، ما قد يتسبب في أضرار لا يمكن إصلاحها. وبإمكان المحتالين من خلال الراوتر المصاب أيضاً، توجيه المستخدمين إلى صفحات تصيّد تتستّر في

هيئة بريد الويب أو مواقع الخدمات المصرفية التي يكثر استخدامها، وبالتالي فإن أية بيانات يُدخلها المستخدمون في هذه الصفحات، سواء كانت بيانات تسجيل الدخول إلى حسابات البريد الإلكتروني أو الحسابات البنكية أو تفاصيل البطاقات المصرفية، ستقع على الفور في أيدي المحتالين.

وارتفع منذ عام 2010 عدد الثغرات الأمنية في أجهزة الراوتر ارتفاعاً مطرداً. وفي عام 2020، ارتفع عدد الثغرات المكتشفة إلى 603، بنحو 3 أضعاف الثغرات المكتشفة في العام السابق. وظل الرقم مرتفعاً في عام 2021 عند 506 ثغرات، بلغ عدد الخطرة منها 87 ثغرة. وتُعتبر الثغرة الأمنية خطرة إذا كانت غير محمية بالمرّة والتي يمكن للمهاجم النفاذ من خلالها لاختراق شبكة منزلية أو مؤسسية. وقد تسمح هذه الثغرات للمهاجم بتجاوز آلية المصادقة أو إرسال أوامر إلى الراوتر عن بُعد أو حتى تعطيله. ويمكن للمهاجمين عند ذلك سرقة أي بيانات أو ملفات تُرسل عبر شبكة مصابة، سواء كانت صوراً أو معلومات شخصية أو أي ملفات ومستندات مهمة مرسلة عبر البريد الإلكتروني.

وتوصي كاسبرسكي المستخدمين باتباع التدابير التالية لحماية أجهزة الراوتر من هجمات المجرمين الرقميين:

ـ شراء الأجهزة الذكية المستعملة يُعتبر ممارسة غير آمنة؛ إذ إن بإمكان مالكيها السابقين تعديل برمجياتها الثابتة لمنحهم القدرة على التحكّم فيها عن بُعد في منزل مشتريها عبر راوتر مُخترق

ـ ضرورة تغيير كلمة المرور الافتراضية التي تأتي مع الراوتر، والحرص على اختيار واحدة معقدة مع تغييرها بانتظام. أو غيرها من المعلومات الحساسة المتعلقة بالأجهزة الذكية على IP ـ الامتناع عن مشاركة الأرقام التسلسلية أو عناوين الشبكات الاجتماعية.

باعتباره الأكثر أمناً لنقل البيانات. WPA2 ـ استخدام تشفير

ـ تعطيل القدرة على الوصول عن بُعد في إعدادات جهاز الراوتر، وإذا كانت هناك حاجة إلى هذه الميزة، فينبغي تعطيلها عند عدم الاستخدام.

(DHCP)« ـ يمكن للمستخدم تحديد عنوان ثابت لبروتوكول الإنترنت، وتعطيل بروتوكول «التهيئة الآلية للمضيف وتتطلب هذه .(MAC) «فضلًا عن حماية شبكة الإنترنت اللاسلكية باستخدام فلتر «عنوان التحكم بالنفاذ للوسط الإجراءات ضبطاً يدوياً لإعدادات العديد من الأجهزة المتصلة بالراوتر، في عملية طويلة ومعقدة، لكنها ستصعّب على مجرمي الإنترنت اختراق الشبكة.

ـ التحقّق دائماً من أحدث المعلومات المتعلقة بالثغرات المكتشفة في أجهزة الراوتر، والتحديثات والتصحيحات البرمجية التي يصدرها المطورون، والمسارعة إلى تثبيتها في الوقت المناسب.

ـ الحرص على تثبيت حل أمني خاص يساعد في حماية الشبكة المنزلية وجميع الأجهزة المتصلة