تنصح بوابة الاتصالات الألمانية "تلتاريف" بضرورة تشفير الشبكة اللاسلكية الخاصة بجهاز الموجه (الراوتر) المنزلي، عن طريق استعمال أحدث معايير التشفير وأكثرها أمانا والمعروفة باسم 2APW؛ وذلك لتحصين الشبكة من هجمات الهاكرز (القراصنة).

وفي حال كان الراوتر قديما لا يدعم هذا المعيار فيمكن تزويده به بشكل لاحق عبر تحديث برنامجه الثابت (فيرموير)، كما أن تحديث البرامج الثابتة بصورة منتظمة مفيد أيضا مع النماذج الحديثة لأنها تعمل على سد الثغرات الأمنية التي يتم اكتشافها. وهناك الكثير من أجهزة الراوتر تتيح للمستخدم إمكانية ضبط وظيفة التحديث التلقائي لبرامج الفيرموير.

وتمتاز أجهزة الراوتر المزودة بفلتر"CAM" بأنها أكثر أماناً، فإذا تم تفعيل هذه الوظيفة فلن تتاح إمكانية تسجيل الدخول في الشبكة المنزلية إلا لأجهزة معينة، ولكن مع هذه الميزة تزيد أعباء إدارة الشبكة نظراً لأنه يتعين على المستخدم إيجاد عنوان "ماك" لكل هاتف ذكي أو حاسوب لوحي أو حاسوب محمول جديد يريد الاتصال بالشبكة المنزلية، ويتم إدخال هذا العنوان في قائمة إعدادات الراوتر.

كما أن إيقاف وظيفة "WPS" يمكن أن يحمي جهاز الراوتر والشبكة المنزلية بصورة أفضل ضد هجمات القراصنة، وذلك لأن وظيفة "WPS" تسهل عملية اتصال أجهزة معينة بالشبكة المنزلية من خلال نقرة واحدة على الزر المخصص لهذه الوظيفة في تلك الأجهزة، ومع ذلك يتعين على المستخدم التخلي عن مثل هذه الوظائف المريحة إذا رغب في زيادة تأمين الشبكة المنزلية ضد هجمات القراصنة.

وفي حال عدم استخدام الراوتر لفترة (كالسفر مثلا) توصي البوابة الألمانية بضبط الراوتر على وضع السكون، حيث يعمل ذلك على حمايته من هجمات القراصنة من ناحية، كما يوفر في استهلاك الطاقة من ناحية أخرى، ويمكن تفعيل هذا الوضع في إعدادات الجهاز التي يمكن الوصول إليها عن طريق متصفح الإنترنت، وغالبا ما يتم تحديد أوقات معينة يتوقف فيها الراوتر عن العمل تلقائيا، مثلا خلال الليل أو عندما لا يكون أحد في المنزل طوال النهار.

كاتب المقالة : منقول
تاريخ النشر : 11/05/2014
من موقع : موقع الشيخ الدكتور/ محمد فرج الأصفر
رابط الموقع : www.mohammdfarag.com