Cyber MSME

Ciberseguridad para PYMES

Consejos de seguridad básicos para nuestro router

Mejora la seguridad de tu red con unos pocos pasos básicos

Creado por CTS Customized Training Solutions &
CASE

Erasmus+

Siguiendo estos sencillos consejos podemos hacer que la red de nuestra Pyme sea más segura:

1. Mire la fecha de fabricación de su router

¿Su router de confianza sigue con usted desde el principio de la empresa? ¿Lo trata como un empleado más? ¡Es comprensible, lo hacemos! Pero cuando está en juego la seguridad de su negocio, no hay lugar para el sentimentalismo.

No existe una regla natural para saber si tenemos que cambiar nuestro dispositivo o no. Los expertos recomiendan reemplazar nuestro router cada 2-3 años, siendo el máximo tiempo sin cambiarlo de 5 años. Debemos cambiar inmediatamente nuestro dispositivo si solo admite un protocolo de cifrado que se sabe tiene importantes vulnerabilidades de seguridad (veremos más adelante más información sobre este tema).

2. Actualice el firmware

¿Comprar un nuevo router, configurar lo básico y no tocar nunca más posteriormente el panel de administración? ¡Todos hemos pasado por ahí! Pero hay buenos motivos para verificarlo de vez en cuando. Los routers, como otros dispositivos conectados a Internet reciben constantes actualizaciones de firmware. Mientras algunos dispositivos hacen esto automáticamente, algunos otros requieren la intervención del administrador para hacerlo – si lo dejamos como está, podemos perder importantes actualizaciones de seguridad, ¡lo que puede ser usado por los maleantes para entrar a nuestra red!

3. Desactivar la configuración de protección del Wi-Fi (WPS)

Cuando visite el panel de administración, acuérdese de apagar el WPS. ¿Qué es el WPS? Es un método para conectar un nuevo dispositivo a la red pulsando un botón del router. Puede parecer útil (¡no tienes que memorizar la contraseña!), pero en realidad es bastante peligroso. ¿Por qué?

El **WPS** es la forma **más común entre los piratas informáticos de obtener acceso no autorizado** a **nuestra** red. Muchas herramientas de hackers se basan únicamente en la explotación del WPS como método para violar la seguridad de su red. **¡Apagarlo es uno de los pasos más fáciles e importantes para mantener su red segura!**

4. No usar protocolos de encriptación WEP o WPA (a menos que tengas que hacerlo)

Al configurar nuestra Wi-Fi nos preguntan si queremos proteger nuestra contraseña (sí queremos) y de ser así, que protocolo de encriptación queremos usar. Este es el momento en que entramos en pánico ya que nos bombardean con enigmáticos acrónimos (WEP, WPA, WPA-PSK, WPA2-PSK, y muchos más). ¿Por qué tantos? ¿Cuál elegir? ¡Respondamos estas preguntas!

Para simplificarlo: los protocolos de encriptación son una manera de autorizar sólo conexiones que precisen de una clave (en nuestro caso, la contraseña del Wi-Fi) y mantener al resto fuera.

WEP fue el primer estándar ratificado y su comienzo se remontan a 1999. Fue reemplazado por WPA (Wi-Fi Protected Access) en 2003, al que siguió WPA2 en 2004. Desde 2018, WPA3 estuvo disponible para su uso.

Entonces, ¿cuál deberías usar? La respuesta simple es **lo más nuevo** que **admita** su router. Si su router solo permite el uso de cifrado WEP o WPA, considere reemplazarlo lo antes posible. Ambos protocolos tienen vulnerabilidades conocidas que permiten a los delincuentes acceder a su red en cuestión de minutos mediante el uso de herramientas disponibles públicamente. WPA2 es el más común en este momento, pero si planea cambiar su router próximamente, compre uno que admita Wi-Fi 6 y WPA3.

Entonces, ¿por qué los "peligrosos" todavía están por aquí? Tenga en cuenta que el dispositivo que se conecta al router también debe poder utilizar el protocolo de cifrado. No es raro que una empresa utilice un dispositivo concreto que solo puede funcionar con un protocolo más antiguo. Si ese es el caso, considere la posibilidad de crear una red adicional para que funcione ese dispositivo para evitar poner en riesgo todos sus dispositivos.

5. Cree una red para invitados aparte

"¿Puedo usar tu Wi-Fi?" es una pregunta que escuchará antes o después si dirige un negocio. Mientras que en el 95% de las veces es una solicitud comprensible (y completamente inocente), nunca hay bastante precaución en lo que respecta a la seguridad, especialmente cuando la mayoría de los dispositivos modernos permiten la creación de una red de invitados con solo pulsar un par de botones. Recuerde: mientras que sus invitados pueden tener la mejor de las intenciones, sus dispositivos pueden estar comprometidos sin ellos saberlo.

6. Pero siempre, siempre, use una contraseña para proteger su red ☺

Si bien todos los consejos anteriores son importantes, este es el más importante. Todos esos pasos no funcionarán si no hay contraseña, como punto de partida ☺ (puede aprender más sobre contraseñas seguras en nuestra herramienta de Buenas Prácticas).

¡Gracias por su atención!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained