Guía del colaborador remoto: Parte 3

Conectividad de la red

Hoy en día, la conectividad se ha vuelto un servicio básico en nuestra vida cotidiana. El acceso a Internet puede hacerse desde diversas locaciones, y existe un amplio rango de opciones gratuitas y hotspots desde donde conectarse.

Pero, así como esta tecnología nos ha dado la posibilidad de trabajar de forma remota, puede también actuar como puerta de entrada para amenazas si los equipos no están correctamente configurados, o si un potencial atacante se encuentra conectado a la misma red. Por este motivo, es preferible utilizar siempre redes seguras para minimizar los riesgos.

¿Qué son redes seguras?

Las redes seguras son aquellas sobre las que se han aplicado varias medidas de seguridad para prevenir la conexión de atacantes o usuarios no autorizados. La más fundamental de estas medidas es simple: **use una contraseña robusta**.

Una red sin contraseña, o con una contraseña débil, puede ser fácilmente accedida por terceros. Por ejemplo, para alguien que posee el conocimiento necesario, es más sencillo obtener una contraseña con cifrado WEP que una con **cifrado de tipo WPA o WPA2** – esta última siendo la más segura y recomendada.

Al tratar con equipos hogareños, es importante que los **routers de Wi-Fi sean inaccesibles por terceros** y tengan contraseñas de administrador fuertes, difíciles de adivinar. Además, es indispensable mantener el firmware del router actualizado y realizar un monitoreo de los equipos conectados a él para prevenir incidentes.

Redes públicas vs. Redes privadas

Las redes públicas son otra cuestión – resultan muy útiles cuando necesita trabajar desde un café, un aeropuerto o cualquier otro espacio público – pero suelen ser redes abiertas ofrecidas como servicio adicional para los clientes. Como tal, dichas conexiones no tienen las medidas de seguridad adecuadas. Si un atacante se conecta a una red pública puede interceptar la información que se transfiere dentro de esa misma red.

Por ello, al conectarse a redes públicas, es importante aplicar las más restrictivas configuraciones de seguridad, especialmente en lo que refiere a archivos compartidos y acceso a sistemas. El mejor consejo es **evitar el uso de servicios que involucren información sensible**.

Gran parte de las compañías utilizan redes privadas que protegen los paquetes de información en tránsito y aseguran una navegación segura a sus usuarios. Pero cuando la conexión de los usuarios es remota, la comunicación va a llevarse a cabo en redes públicas e inseguras. Las organizaciones deberán establecer un protocolo EGP (*Exterior Gateway Protocol*) que posea controles adicionales, y medidas para proteger tanto la red interna de la compañía como la comunicación con los equipos de los empleados remotos.

En ocasiones utilizamos redes que no pertenecen a nuestra conexión hogareña ni tampoco a una pública – suele ser alguna red de terceros, como de un hotel o casa de algún amigo. Si bien estas redes son privadas, el usuario no sabe quién más está conectado a ellas, ni cuáles son sus intenciones. Por este motivo, incluso si conoce y confía en el administrador, deberían tomarse las mismas precauciones que con las redes públicas.

VPN

Las Redes Privadas Virtuales (VPN, por sus siglas en inglés) son una tecnología que cifra las comunicaciones en una red para **ofrecerle acceso remoto seguro a una red privada**.

Si bien hay varios protocolos disponibles para conectarse a través de una VPN, todos utilizan el cifrado para transportar información y que resulte ilegible hasta llegar a destino. De esta manera, si los atacantes interceptaran su comunicación, no serían capaces de leerla o utilizarla.

Muchas compañías proveen a sus empleados de conexiones VPN para conectarse de forma remota a servicios e información de la red interna. Ya que estos tipos de conexión incluyen cifrado, también es recomendable utilizar una VPN cada vez que se realice una conexión a una red pública o insegura.

¿No cuenta con un departamento de IT para configurar una VPN para su negocio? Acceda a la guía de teletrabajo para empresas, disponible en WeLiveSecurity.

Doble Factor de Autenticación

El Doble factor de autenticación (2FA), **es una tecnología que complementa la autenticación tradicional para acceder a los servicios**. Aparte de utilizar un usuario y contraseña, se requiere información adicional para habilitar el ingreso. Esta podría ser un código de seguridad, un token o cualquier otra cosa que el usuario posea.

En general se genera un código, disponible mediante SMS, una app de autenticación (más seguro), o incluso a través de algo tan simple como una llave de seguridad USB.

El objetivo del 2FA es proteger el acceso a sus cuentas y dispositivos en casos en los que su contraseña se vea comprometida. Esto puede suceder ya sea por un código malicioso, una infiltración en los sistemas IT de su compañía o a través de un engaño.

El trabajo remoto aumenta el riesgo de que un atacante pueda robar sus credenciales. Al añadir un segundo factor de autenticación, los intentos del atacante de usar su contraseña para ingresar se verán frustrados. ESET ofrece a los negocios una solución de 2FA integral, mediante ESET Secure Authentication.

En la cuarta parte de esta serie, veremos cómo preparar a sus empleados para que reciban soporte técnico remoto y daremos fin al ciclo con un resumen de prácticas recomendadas.