GUÍA DE CONTROLES DE SEGURIDAD DE REDES DE HOGAR (20/OCTUBRE/2021)

En la actualidad las redes de comunicaciones del hogar se han convertido en la infraestructura de soporte para la realización de actividades cotidianas de los integrantes de una familia, que comprenden ámbitos laborales, educativos y escolares. En este sentido el EcuCERT considera que es necesario realizar actividades de control y mitigación de riesgos en al menos los parámetros descritos en esta guía, a fin de poder precautelar la seguridad de los activos de información que son gestionados a través de las redes de comunicaciones del hogar.

Routers

Las contraseñas de los dispositivos *router* deben ser cambiadas por los usuarios evitando utilizar las credenciales que vienen por defecto.

Wifi

Los dispositivos wifi que son los que garantizan la movilidad de los usuarios y la cobertura dentro de la red de hogar, deben tener activado los protocolos de cifrado seguro.

Actualización de Sistemas Operativos

Los sistemas operativos son considerados como elemento estratégico en la seguridad de un sistema de información, ya que el mismo controla el uso y

acceso a los recursos de software y hardware. Los sistemas operativos deben mantenerse actualizados y los parches de seguridad instalados.

Actualización de las aplicaciones

Es necesario que, todas las aplicaciones utilizadas y existentes en los dispositivos de información sean periódicamente actualizadas, cubriendo así los errores y fallas de programación, que por lo general se presentan en aplicaciones que no tienen por objetivo principal las funcionalidades de seguridad, sino más bien el interés de operatividad por parte de los usuarios. Es necesario analizar la pertinencia de mantener activada la opción de actualización automática.

Contraseñas seguras

Debido al número de dispositivos de comunicación y aplicaciones que cada usuario accede dentro de una red de hogar, los usuarios tienden a utilizar las mismas credenciales, lo cual implica un alto riesgo en caso de que por una falla de seguridad sean filtradas. Por tanto, es necesario que las contraseñas mantengan un alto nivel de seguridad y no se utilicen las mismas credenciales para cada dispositivo o aplicación a la que accedemos.

Cortafuegos - Firewall

Por lo general los dispositivos de comunicaciones tienen funcionalidades de seguridad para evitar conexiones maliciosas. Los firewalls permiten la restricción de origen y destino de las comunicaciones a establecerse en un dispositivo. Es necesario activar incluso las configuraciones por defecto de estas funcionalidades, y así prevenir ataques.

Respaldos de seguridad

Ante la *imposibilidad de garantizar totalmente la seguridad* de los dispositivos y sistemas de información, es necesario generar de manera periódica respaldos o copias de seguridad, que permitan garantizar la continuidad de las actividades cotidianas aun ante la ocurrencia de un incidente de seguridad.

Referencias

- Oficina de Seguridad del Internauta, 2017. Te refrescamos cómo proteger la red wifi de casa. Disponible en https://www.zdnet.com/article/meris-botnet-assaults-krebsonsecurity/.
- Kaspersky, 2018. 5 consejos para proteger tu red doméstica. Disponible en https://latam.kaspersky.com/blog/secure-your-home-network/13547/