Publicado en Madrid el 21/11/2019

S2 Grupo aporta nueve claves para ciberproteger dispositivos IoT

Debido a que cada año en la celebración del Black Friday hay un incremento en la compra de artículos IoT, el equipo de expertos de S2 Grupo ha elaborado un decálogo con recomendaciones esenciales para proteger adecuadamente los "aparatos inteligentes"

S2 Grupo, empresa especializada en ciberseguridad y gestión de sistemas críticos, ha advertido de que la proliferación en los hogares de dispositivos IoT (Internet de las Cosas) requiere un incremento de la concienciación de las familias para promover la protección de estos aparatos conectados y, de ese modo, proteger su privacidad.

“Cada vez son más las familias donde hay smart TV, bombillas inteligentes, cámaras de vigilancia conectadas, enchufes inteligentes, altavoces inteligentes, etc. Esto es fantástico, porque aportan un valor y una funcionalidad en el día a día, pero hay que ser conscientes de que también supone un incremento de la exposición de los hogares a posibles injerencias de terceros”, ha explicado José Rosell, socio-director de S2 Grupo.

“Dejar la configuración que viene por defecto en estos dispositivos, hacerlo de forma inadecuada o no mirarla siquiera, puede conllevar problemas graves para la seguridad de los hogares y su privacidad si son víctimas de los ciberdelincuentes. El objetivo de éstos suele ser económico, porque la información privada mueve muchísimo dinero en sus entornos. Esto puede ser desde robo de claves, de datos de tarjetas, de fotografías, vídeos o información de las empresas en las que trabajan, por ejemplo”, ha asegurado Miguel A. Juan, socio-director de S2 Grupo.

En este contexto y, vaticinando que de cara a la próxima celebración del Black Friday cada año se vive un incremento en la compra de artículos IoT, el equipo de expertos de S2 Grupo ha elaborado un decálogo de recomendaciones esenciales para proteger adecuadamente estos dispositivos:

Comprobar la configuración de la red Wi-Fi. El router tiene que disponer de contraseña robusta (y haber cambiado el nombre y la contraseña que aparecen por defecto) para evitar que terceras personas puedan conectarse a la red y a los aparatos sin permiso.

Revisar las contraseñas de acceso a los dispositivos. Es fundamental cambiar las contraseñas y el usuario de acceso que vienen de serie, ya que estos datos son fácilmente localizables en la red o simplemente teniendo el mismo artículo.

Utilizar contraseñas diferentes para cada dispositivo. Si se usan claves distintas a las de otros servicios de Internet, por ejemplo, incrementará la ciberseguridad. Esto se fundamenta en que si, por algún motivo, alguien se da de alta en algún espacio que resulta comprometido para la acción de los ciberdelincuentes, no pondrá en peligro el resto de sus aparatos conectados.

Revisar que las contraseñas sean robustas. Es decir, tienen que contar con mayúsculas, minúsculas, números y símbolos intercalados; y nunca deben incluir información personal, como la fecha de un cumpleaños, por ejemplo.

Revisar los ajustes de privacidad y seguridad. Casi todos los artículos conectados cuentan con un menú de “configuración” en sus aplicaciones o en la web que los administran desde donde se puede hacer un ajuste de la privacidad y seguridad. De esta forma, se podrá evitar que obtengan información con fines comerciales. Por ejemplo, los asistentes de voz suelen guardar un historial de entradas de audio cuando se interactúa con ellos y ese historial puede ser consultado o borrado.

Activar las actualizaciones automáticas en los dispositivos inteligentes. Esto es clave para que estén cubiertos contra posibles agujeros de seguridad.

Activar la opción de búsqueda de antivirus. Algunas Smart TVs cuentan con esta función y es interesante que lo realicen periódicamente.

Revisar las aplicaciones o skills de los dispositivos IoT. De la misma manera que en los teléfonos móviles o tablets, al instalar una nueva opción se le otorgan permisos a la misma, en la configuración de los aparatos IoT se podrán revisar y desactivar los que no interesen.

Descargar nuevas funcionalidades para los dispositivos IoT sólo desde tiendas oficiales. Hacerlo desde otros lugares puede ser la causa de una infección por malware.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Software Ciberseguridad Consumo Dispositivos móviles