OUCH! | Agosto 2018

OUCH!

SANS SECURITY AWARENESS

Boletín mensual de seguridad para todos

Dispositivos en hogares inteligentes

¿Qué son los dispositivos de hogares inteligentes?

Tradicionalmente, solo algunos de tus dispositivos en casa podían conectarse a Internet, como tu laptop, tu teléfono móvil o tu consola de videjuegos. Sin embargo, hoy en día cada vez más dispositivos están conectados a la red, desde las bombillas hasta los altavoces de la TV, los seguros de las puertas e incluso tu auto. Muy pronto, casi todos los dispositivos en tu hogar podrán conectarse a Internet. Estos dispositivos conectados a menudo se conocen como Internet de las cosas o dispositivos de hogares inteligentes. Mientras estos dispositivos conectados traen bastante comodidad, también implican peligros particulares.

¿Cuál es el problema?

Entre más dispositivos estén conectados a la red de tu hogar, más problemas puede haber. Los ciberatacantes pueden programar tus dispositivos para atacar a otros, los fabricantes pueden recolectar bastante información sobre tus actividades o tus dispositivos pueden ser infectados de manera que no puedas acceder a ellos. Muchas de las compañías que fabrican estos aparatos no tienen experiencia con la ciberseguridad y ven a la seguridad como un costo. Como resultado, muchos de los dispositivos que adquieres tienen muy poca o nada de seguridad incluida. Por ejemplo, algunos dispositivos tienen contraseñas por defecto que son bien conocidas o no pueden ser actualizados ni modificados en su configuración.

¿Cómo me puedo proteger?

Así que, ¿qué puedes hacer? Definitivamente queremos que aproveches los dispositivos conectados, de manera cautelosa y segura. Estos dispositivos pueden ofrecer maravillosas funciones para facilitar tu vida. Adicionalmente, conforme avanza la tecnología puede ser que no tengas otra opción que de usar dispositivos inteligentes. Aquí encontrarás pasos clave que puedes tomar para protegerte a ti mismo.

Conecta solo lo que necesitas: La manera más simple de asegurar un dispositivo es no conectarlo a Internet. Si no necesitas que el dispositivo esté en línea, no lo conectes a tu red Wi-Fi. ¿En serio necesitas que tu tostadora te envíe notificaciones al móvil?

Conoce lo que está conectado: ¿Qué dispositivos tienes conectados a tu red? ¿No estás seguro o no lo recuerdas? Apaga tu red inalámbrica y averigua qué deja de funcionar. Puede ser que no detectes todo, pero te sorprenderás de cuántos dispositivos olvidaste.

Mantente actualizado: Como en el caso de tu computadora y dispositivos móviles, es crítico que mantengas actualizados todos tus dispositivos. Si tu aparato tiene la opción de actualizarse automáticamente, actívalo.

Contraseña: Cambia las contraseñas en tus dispositivos por una frase de contraseña única y fuerte que solo tú conozcas. Es probable que solo tengas que usarla una vez. ¿No puedes recordar todas tus frases de contraseña? No te preocupes, nosotros tampoco. Considera usar un gestor de contraseñas para asegurar todas ellas.

Opciones de privacidad: Si tu dispositivo te permite configurar tus opciones de privacidad, limita la cantidad de información que colecta o comparte. Una opción es deshabilitar la capacidad de compartir información.

Fabricante: Compra tus dispositivos con una compañía que conozcas y en la que confíes. Busca productos que tengan medidas de seguridad, como permitir la actualización automática o cambiar la contraseña por defecto y modificar la configuración de privacidad.

Siempre escuchando: Si un dispositivo puede captar tus órdenes por medio de la voz, entonces está escuchando constantemente. Por ejemplo, los dispositivos Alexa y Google Home pueden grabar conversaciones sensibles. Considéralo cuando determines dónde colocar los dispositivos en tu casa, y revisa las opciones de privacidad.

Red de invitados: Considera usar una red Wi-Fi de invitados para los dispositivos de hogares inteligentes, en lugar de usar la red principal que utilizas para tus computadoras y dispositivos móviles. De esta manera, si cualquier dispositivo inteligente es infectado, tus computadoras y móviles en la red principal estarán a salvo.

No hay razón para temer a las nuevas tecnologías, pero sí se debe comprender el riesgo que presentan. Al seguir estos simples pasos puedes ayudar a crear un hogar inteligente mucho más seguro.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor Invitado

Robert M. Lee *(@RobertMLee) es instructor certificado por SANS y autor de FOR578: Inteligencia de Ciberamenazas y ICS515: Defensa activa y respuesta a incidentes. Robert también es CEO y fundador de la firma de ciberseguridad industrial Dragos.*

Recursos

Frase de contraseña:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_sp.pdf
Gestores de contraseñas:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_sp.pdf
Asegurando tu red doméstica:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201602_sp.pdf