Comunicado de Prensa
No.029/2024

Ciudad de México, a 9 de abril de 2024.

EL IFT PUBLICA EL ANÁLISIS DE CIBERSEGURIDAD EN LOS DISPOSITIVOS DE INTERNET DE LAS COSAS (IoT)

- ***Se realizó un análisis a 348 fabricantes o marcas de dispositivos IoT que se comercializan en México y se encuentran homologados en el IFT, tomando como referencia el Código de mejores prácticas para la ciberseguridad del Internet de las Cosas.***
- ***Del total de las marcas analizadas, 8% no cuenta con ningún tipo de información relacionada con las características de ciberseguridad de sus dispositivos.***
- ***Algunas de las marcas revisadas en sus términos, condiciones y avisos de privacidad no incluyen información respecto a los incidentes de seguridad relacionados con la información y datos personales de los usuarios.***
- ***En algunas ocasiones, no existe información ni página web para consultar información de seguridad en los dispositivos.***

El Instituto Federal de Telecomunicaciones (IFT) publicó el análisis "Ciberseguridad en los dispositivos de Internet de las Cosas (IoT)", en el que se dan a conocer los resultados del análisis a 348 fabricantes o marcas, que tienen dispositivos homologados y que pueden ser consultados en el Catálogo de Dispositivos IoT que se publicó el 21 de diciembre de 2022 y que está disponible en la página de internet de este órgano regulador.

El documento tiene como objetivo transparentar la información que los fabricantes o marcas difunden en sus portales de internet y que se encuentra asociada a las características que se establecen en el Código de mejores prácticas para la ciberseguridad del Internet de las Cosas, publicado por el IFT en febrero de 2023.

Para la integración del análisis, el IFT realizó una clasificación de los controles técnicos y políticas organizativas que se sugiere observen los fabricantes de los Dispositivos IoT, en el Código de mejores prácticas para la ciberseguridad del Internet de las Cosas.

Posteriormente, se clasificó la información agrupada en las fichas organizativas conforme a los siguientes apartados:

• Contraseñas.
• Actualizaciones al software.
• Sobre el uso de comunicaciones seguras.
• Integridad del software.
• Sobre los datos de telemetría.
• Sobre la eliminación de los datos personales.
• Sobre las credenciales y los parámetros de seguridad sensible.

Del análisis se obtuvieron los siguientes hallazgos:

1. La información sobre especificaciones de ciberseguridad en los productos de algunas de las marcas revisadas no fue de fácil ubicación, ya que en sus páginas web es necesario realizar una búsqueda exhaustiva.
2. Algunas de las marcas revisadas en sus términos, condiciones y avisos de privacidad no incluyen información respecto a los incidentes de seguridad relacionados con la información y datos personales de los usuarios.
3. En algunas ocasiones no existe información ni página web para consultar información de seguridad en los dispositivos.
4. En algunos casos, los términos, condiciones y avisos de privacidad de las marcas revisadas se encuentran en idiomas distintos al español.
5. Del total de las marcas analizadas, el 8% no cuenta con ningún tipo de información relacionada con las características de ciberseguridad de sus dispositivos.

Con la finalidad de promover la confianza y el uso seguro de estas nuevas tecnologías, resulta importante tomar en cuenta las siguientes recomendaciones:

- Verifica si las actualizaciones de software de tu dispositivo se realizan de manera automática o no, y procura mantenerlo actualizado.
- Personaliza el nombre de usuario y contraseña del dispositivo y/o la cuenta asociada.
- Utiliza contraseñas seguras para acceder a tu dispositivo y la cuenta asociada.
- Si es posible, además de las contraseñas seguras, utiliza un método de doble autenticación para acceder a tu dispositivo y la cuenta asociada. Revisa el tratamiento que le darán a tu información y datos personales.
- Cuando no estés haciendo uso del dispositivo, desactívalo.
- Si ya no utilizarás el dispositivo, elimina tu información y datos personales almacenados en este, así como la cuenta asociada.
- Identifica la información que tus equipos recolectan y los mecanismos que tienen habilitados para configurar la privacidad. Utiliza los mecanismos de configuración de privacidad con la finalidad de que solo sea visible la información que desees.

Actualmente, las personas comparten su información a través de un número creciente de dispositivos IoT y servicios asociados en línea que permanentemente están recolectando y procesando dichos datos. Por lo anterior, es importante promover el uso informado de los dispositivos y la concientización sobre los datos que se recolectan y los riesgos que esto conlleva.

Por ello, resulta importante que los dispositivos sean diseñados para resistir amenazas en la seguridad, ya que los riesgos vinculados a una falla o falta de seguridad en estos aparatos conectados a internet afecta la confianza, privacidad y economía de quienes los usan.

El análisis se puede consultar en la siguiente liga:
https://ciberseguridad.ift.org.mx/files/guias_y_estudios/ciberseguridad_de_los_dispositivos_iot.pdf

Comunicado de Prensa
No.029/2024

----------**********----------

El Instituto Federal de Telecomunicaciones (IFT) es el órgano autónomo encargado de regular, promover y supervisar el desarrollo eficiente en los sectores de radiodifusión y telecomunicaciones en México, además de ejercer de forma exclusiva las facultades en materia de competencia económica en dichos sectores, de conformidad con el Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6, 7, 27, 28, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones, publicado en el Diario Oficial de la Federación el 11 de junio de 2013.

Coordinación General de Comunicación Social
Insurgentes Sur 1143 1er. Piso, Col. Nochebuena,
Benito Juárez. C.P. 03720
Tels. 55 50 15 40 00 ext. ext. 2280 y 4548

INGRESA A NUESTRO PORTAL: WWW.IFT.ORG.MX

/IFT.mx @IFT_MX iftmexico IFTmx iftmexico