Wearables: ¿son un riesgo para la privacidad?

Los relojes inteligentes, dispositivos de monitoreo de actividad física y otros tipos de wearables, se están volviendo casi comunes como los teléfonos móviles y tabletas. Estos gadgets conectados, monitorean la salud, permiten revisar el correo electrónico, controlar los hogares inteligentes e incluso se pueden utilizar para realizar pagos. Son una extensión de lo que se conoce como dispositivos de la Internet de las Cosas (IoT, por sus siglas en inglés) que intentan que la vida diaria sea más saludable y cómoda al reducir el tiempo de exposición a la pantalla de los teléfonos, que en países como Estados Unidos alcanzó un promedio de casi seis horas este año.

Es un mercado que se espera que en los próximos años tenga un crecimiento de 12,5% anual, para superar los 118 billones de dólares en 2028. No obstante, si bien los wearables están siendo parte de la vida cotidiana, también recopilan más datos y se conectan a un número cada vez mayor de otros sistemas inteligentes. Es por eso que ESET, compañía líder en detección proactiva de amenazas, analiza los posibles riesgos de seguridad y privacidad que se puede encontrar alrededor de esta tecnología.

"Los actores de amenazas tienen múltiples formas de monetizar los ataques a los wearables inteligentes y al ecosistema relacionado de aplicaciones y software. Podrían interceptar y manipular datos y contraseñas y desbloquear dispositivos perdidos o robados. También existen posibles preocupaciones de privacidad sobre el intercambio encubierto de datos personales con terceros", comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Las principales **preocupaciones respecto a la seguridad y privacidad según ESET,** son:

1. **Robo y manipulación de datos:** Algunos de los relojes inteligentes con más funciones proporcionan acceso sincronizado a las aplicaciones de tu smartphone, como el correo electrónico y apps de mensajería. Esto puede llevar a que usuarios no autorizados intenten interceptar datos personales y confidenciales de los usuarios. Otro aspecto igualmente preocupante es dónde se almacena gran parte de esos datos. Si no está debidamente protegido el proveedor puede ser blanco de atacantes que buscan robar información. Hay un mercado clandestino muy próspero para ciertos tipos de datos personales y financieros.
2. **Amenazas basadas en la ubicación:** Otro tipo de datos clave registrados por la mayoría de los wearables se relaciona con la ubicación. Con esta información los ciberdelincuentes pueden construir un perfil preciso de sus movimientos a lo largo del día. Eso podría permitirles atacar físicamente al usuario, o a su automóvil o a su hogar si, por ejemplo, se tiene la información de que están vacíos. Hay preocupaciones aún mayores sobre la seguridad de los niños que usan tales dispositivos, si están siendo rastreados por terceros no autorizados.

3. **Compañías terceras:** No son solo los riesgos de seguridad a lo que los usuarios deben prestar atención y estar alerta. Los datos que recopilan los dispositivos pueden ser

extremadamente valiosos para los anunciantes. Y hay una demanda importante de tales datos en ciertos mercados. Un informe aseguró que los ingresos obtenidos a partir de los datos vendidos por los fabricantes de dispositivos de salud a las compañías de seguros podrían alcanzar los 855 millones de dólares para 2023.

Algunas de estas compañías pueden incluso utilizar los datos para crear perfiles publicitarios de los usuarios y venderlos. Si estos datos son almacenados por varias otras empresas, el riesgo a una posible brecha es mayor.

4. Desbloqueo de un hogar inteligente: Ciertos wearables podrían usarse para controlar dispositivos IoT de un hogar inteligente. Incluso podrían configurarse para desbloquear la puerta de tu casa. Esto presenta un riesgo de seguridad importante en caso de que los dispositivos se pierdan o sean robados y la configuración antirrobo no esté habilitada.

Además, según ESET hay múltiples elementos que forman parte del dispositivo que son susceptibles de recibir ataques si la seguridad y la privacidad no han sido consideradas adecuadamente por el fabricante. Desde el firmware del dispositivo hasta los protocolos que utiliza para la conectividad, sus aplicaciones y servidores backend en la nube. Estos son algunos ejemplos:

- Bluetooth: Bluetooth Low Energy se utiliza típicamente para emparejar dispositivos portátiles con el teléfono inteligente. Pero se han descubierto numerosas vulnerabilidades en el protocolo a lo largo de los años que podrían permitir a atacantes cercanos bloquear dispositivos, espiar o manipular datos.

- Dispositivos: A menudo el software en el propio dispositivo es vulnerable a ataques externos debido a un desarrollo deficiente. Incluso un reloj inteligente bien diseñado es construido por humanos y, por lo tanto, puede contener errores en el código. Estos también pueden conducir a filtraciones que comprometan la privacidad, pérdida de datos y más. Una autenticación/cifrado débil en los wearables puede significar exponerlos al secuestro y a la escucha indebida. Además, los usuarios también deben ser conscientes de quienes espían si están viendo mensajes/datos confidenciales en sus dispositivos portátiles en lugares públicos.

- Aplicaciones: Las aplicaciones de los teléfonos inteligentes vinculadas a los wearables son otra vía de ataque. Pueden haber sido programados deficientemente y estar plagados de vulnerabilidades que exponen los datos y el dispositivos del usuario. Otro riesgo es que las aplicaciones, o incluso los propios usuarios, sean descuidados con los datos. También puede ocurrir que el usuario descargue accidentalmente aplicaciones falsas diseñadas para parecerse a las legítimas y que los atacantes roben información personal que han ingresado en ellas.

- Servidores back-end: Los proveedores de sistemas basados en la nube pueden almacenar información del dispositivo, incluidos datos de ubicación y otros detalles. Eso representa un objetivo atractivo para los atacantes. No hay mucho que se pueda hacer al respecto, aparte de elegir un proveedor de buena reputación con un buen historial de seguridad.

“Las preocupaciones entorno a los wearables persisten hasta el día de hoy, con investigaciones que

muestran dispositivos susceptibles de manipulación que incluso podrían causar angustia física al usuario. Otro estudio afirmó que los cibercriminales podrían cambiar contraseñas, hacer llamadas, enviar mensajes de texto y acceder a cámaras desde dispositivos diseñados para monitorear a adultos mayores y niños. A medida que los dispositivos portátiles se conviertan en una parte cada vez más importante de todas nuestras vidas, se convertirán en un objetivo más grande para los atacantes. Investigar antes de comprar y cerrar tantas vías de ataque como sea posible una vez que se inicie el dispositivo es clave para la protección", agrega Camilo Gutierrez Amaya de ESET.

Para minimizar los riesgos, ESET comparte hay varios:

- Activar la autenticación en dos pasos
- Proteger con contraseña las pantallas de bloqueo
- Cambiar la configuración para evitar cualquier emparejamiento no autorizado
- Solo visitar tiendas de aplicaciones legítimas
- Mantener todo el software actualizado
- Nunca hacer jailbreaking/rootear dispositivos
- Limitar los permisos de las aplicaciones
- Contar con una solución de seguridad instalada en el dispositivo
- Elegir proveedores de wearables de buena reputación
- Examinar de cerca los ajustes de privacidad y seguridad para asegurarse de que están configurados correctamente

Proteger el hogar inteligente al:

- No sincronizar dispositivos portátiles con la puerta de la casa
- Mantener los dispositivos en la red Wi-Fi de invitado
- Actualizar de todos los dispositivos al firmware más reciente
- Asegurarse de modificar todas las contraseñas predeterminadas de fábrica que vengan en los dispositivos