Los riesgos asociados a los dispositivos IoT

En los últimos años, el Internet de las Cosas (IoT) ha pasado de ser un concepto futurista a convertirse en una realidad. Check Point, la firma especializada en ciberseguridad, señala que, a pesar de sus múltiples ventajas y el amplio abanico de ámbitos de aplicación que tienen estos dispositivos, estas innovaciones vienen acompañadas de múltiples amenazas que ponen en **riesgo los niveles de ciberseguridad de usuarios y compañías de todo el mundo**.

Para Eusebio Nieva, director técnico de Check Point para España y Portugal, los automóviles, vehículos, electrodomésticos, relojes, entre muchos otros más dispositivos conectados a internet que están siendo usados en empresas y oficinas, deben protegerse correctamente o podrían abrirse vulnerabilidades que pueden ser usadas por ciberdelincuentes.

"**La mayoría de los dispositivos IoT cuentan con niveles de protección muy bajos** o prácticamente inexistentes, puesto que se diseñan pensando en su funcionalidad, dejando de lado la importancia de la seguridad. Por tanto, este tipo de dispositivos son muy vulnerables frente a las ciberamenazas más avanzadas, lo que afecta tanto a usuarios como a empresas", añade Nieva.

Entre los riesgos más comunes asociados a los dispositivos IoT se encuentran el acceso al resto de la red: los electrodomésticos, especialmente las neveras o los televisores, son los últimos ejemplos de una larga lista de productos que se han incorporado al tejido de dispositivos conectados a internet.

"Sin embargo, **su incorporación al mundo digital no ha venido acompañada de un aumento en los niveles seguridad frente a potenciales ciberataques**. Por tanto, se convierten en puntos débiles dentro de la red de dispositivos conectados, por lo que un cibercriminal puede aprovecharse de este punto de acceso y emplearlo como puente para comprometer la seguridad de otros elementos conectados a la red como ordenadores, teléfonos, etc.", agregó Nieva

Otro factor es el espionaje a través del smartwatch. Los relojes inteligentes y las pulseras de actividad física están equipados con una gran variedad de sensores que les permiten desarrollar sus funcionalidades como ubicación por GPS, contar los pasos, medir el pulso, etc.

"Estos dispositivos recaban una gran cantidad de información que hace posible identificar patrones de comportamiento, períodos de tiempo, cuándo y dónde se mueven los usuarios y durante cuánto tiempo. De esta forma, si la seguridad de cualquiera de estos dispositivos se viera comprometida, un cibercriminal podría utilizarla para inmiscuirse en nuestro ámbito privado o profesional", explicó el director técnico de Check Point.

Más cuidados

El **robo de datos a través de las Smart TVs** es otro de los riesgos reportados. Una buena parte de los usuarios utiliza aplicaciones de reproducción de video en streaming o de reproducción de música, entre otros, directamente desde su televisión inteligente.

"Para ello, es necesario que introduzcan sus credenciales, algo que supone un riesgo teniendo en cuenta el bajo nivel de protección de estos dispositivos. Además, esto supone una amenaza aún

mayor si tanto el usuario como la contraseña son los mismos para otros servicios como por ejemplo el correo electrónico", comenta Nieva.

Por este motivo, desde Check Point aconsejan no utilizar la misma contraseña en distintas plataformas.

Los avances en las Smart Cities también vienen marcados por la evolución que experimentan los automóviles, no sólo en lo relativo a su fuente de energía, sino también a la conectividad, ya que cada vez más vehículos cuentan con funcionalidades conectadas a la red.

En este sentido, cabe destacar que poco a poco se van viendo los primeros coches autónomos que cuentan con infinidad de sensores que permiten calcular la distancia con todos los elementos que se encuentran a su alrededor, control de velocidad y freno, etc. Por tanto, **un ciberdelincuente podría tomar el control de uno o varios de estos vehículos y provocar colisiones o robar los vehículos**.

"La implantación de la tecnología con el objetivo de mejorar y facilitar nuestras vidas es un hecho. Vivimos rodeados de dispositivos conectados a internet que tienen acceso a nuestros datos, pero tendemos a infravalorar los riesgos que pueden suponer para la seguridad. Por este motivo, desde Check Point somos conscientes de la necesidad de ofrecer soluciones capaces de cubrir cada vez más dispositivos, así como **apostamos por inculcar en la sociedad una cultura basada en el uso de soluciones de ciberseguridad** que garanticen que nuestra información y nuestros sistemas estén a salvo en todo momento", agrega Nieva.