Prestando atención a nuestros dispositivos IoT

El Internet de las cosas está aquí y crece cada día.. Es una realidad a la que hay que prestar atención, ya que, además de muchas oportunidades, trae consigo muchos riesgos tanto para las empresas como para las personas.

Si recordamos el post anterior, en el que hablábamos de los riesgos de IoT, decíamos que dichos riesgos están mayormente relacionados con la ciberseguridad, por desconocimiento, por falta de concienciación, por despreocupación, etc. Los riesgos son tan reales como la tecnología que tenemos delante. Sobre todo las empresas debería empezar a concienciarse y concienciar a sus empleados y colaboradores de que es necesario contemplar muchos aspectos relacionados con IoT. Deberían empezar por preguntarse [1]:

- ¿Cómo se implementa el IoT en la organización? ¿El inventario potencial de IoT? ¿La tecnología IoT es parte de su producto?
- ¿Han considerado los riesgos asociados a IoT? ¿Se han cuantificado o controlado? ¿Se considera IoT al aplicar políticas o prácticas de datos y privacidad y se evalúa la seguridad?

- ¿Saben qué datos se recopilan, almacenan y analizan? ¿Se han evaluado las implicaciones legales, de privacidad y seguridad relacionadas?
- ¿Tienen planes de contingencia para “cosas” conectadas que sean infectadas? ¿Se ha evaluado el uso de tecnologías IoT, y cuál sería su impacto si se desconectaran? ¿Se considera el IoT en los planes de gestión de la continuidad del negocio? ¿Y si es importante el IoT, qué procedimientos hay para su recuperación en caso de catástrofe?
- ¿En qué medida actúan terceros en nuestro nombre con respecto a tecnologías IoT? ¿Existen procesos y acuerdos para monitorearlos? ¿Se monitorean los datos capturados y enviados a través de proveedores de servicios externos?
- ¿Qué rol juega el IoT en la estrategia actual de la empresa? ¿Tienen una estrategia de IoT? ¿Se evalúa el impacto del IoT?
- ¿Cuál es el riesgo de no considerar o aprovechar las posibilidades del IoT? ¿Cuál es el riesgo si ignoramos el IoT?

Estas preguntas debieran hacérselas tanto proveedores como consumidores de IoT. Debemos saber perfectamente qué supone IoT para nosotros y cómo nos estamos relacionando con él. Es importante tener claro qué riesgos concretos suponen para nosotros estas tecnologías. Una vez tengamos claro esto, debemos elaborar un plan de contingencia y tomar medidas para mitigar dichos riesgos.

Como decíamos, el principal riesgo al que hay que prestar atención, es la ciberseguridad. Para mitigar este riesgo, y evitar que un malware como Mirai nos afecte, debemos ser cuidadosos, en primer lugar, al escoger nuestros proveedores de IoT, con nuestros productos siendo proveedores de IoT y siendo consumidores de un dispositivo IoT; y en segundo lugar, sabiendo perfectamente qué dispositivos IoT manejamos y

tenemos conectados a nuestra red.

Es necesario que nuestro proveedor o nosotros como proveedores de IoT, hagamos las preguntas correctas y se mantenga nuestro producto siempre seguro mediante actualizaciones de seguridad.

Una vez dispongamos de un dispositivo IoT debemos cambiar las credenciales predeterminadas de nuestro dispositivo, utilizar contraseñas robustas, mantener su firmware actualizado, deshabilitar las características o funcionalidades que no vayamos a utilizar, apagar su conectividad si no la estamos utilizando y si la usamos verificar que el panel de administración no está accesible desde internet, segmentar la red para los dispositivos IoT conectados si no necesitan estar en la misma red que el resto de dispositivos, deshabilitar o proteger el acceso remoto a nuestro dispositivo mientras no sea necesario e investigar y aprovechar las medidas de seguridad que ofrece nuestro dispositivo [2].

Esto es importante porque lo que estamos poniendo sobre la mesa es nuestra información. Lo que nos lleva al segundo riesgo importante que comentábamos en el post anterior: la privacidad.

A día de hoy, la información es un activo muy importante tanto para las empresas como para las personas. Por este motivo debemos tener siempre el control de nuestros datos, saber qué datos se recogen, para qué fin se están recogiendo y cómo se van a utilizar esos datos.

Demasiadas son las veces que como usuarios pasamos las políticas de privacidad por alto. Si nos detuvieramos a leer cada una de ellas (a parte de que tardaríamos muchísimo tiempo debido a su extensión y lenguaje farragoso en su mayoría), lo más probable es que no quisiéramos aceptar ni la mitad.

Desde el navegador de nuestro ordenador se recogen multitud de datos, desde nuestro móvil se recogen otro tantos, desde cualquier dispositivo IoT se pueden recoger muchísimos datos

sobre nosotros. Datos sobre nuestras costumbres, gustos, aficiones, etc. Por eso debemos tener cuidado con las preferencias de seguridad y privacidad de todos nuestros dispositivos si no queremos que se recojan y utilicen muchos de esos datos.

Referencias:

[1] The Internet of Things: What Is and Why Should Internal Audit Care? – Protiviti, 2017 https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/arttheinternetofthings

[2] Recomendaciones de Seguridad en Dispositivos IoT – Carlos Capdevila, 2017 https://www.ithinkupc.com/blog-es/recomendaciones-de-seguridad-en-dispositivos-iot

[3] 5 Maneras de Gestionar Riesgos de Movilidad e IoT – Aruba https://www.arubanetworks.com/assets/_es/wp/WP_5_Ways_to_Manage_Mobility_And_IoT_Risks.pdf