Más riesgos y cierre

Introducción

Durante esta lista de posts he ido hablando sobre diversos temas relacionados con el IoT. En el primero artículo introduje un poco el tema sobre los dispositivos conectados a la red. Durante el segundo hablé de las aplicaciones que tiene esta tecnología en la industria. Los últimos 2 post han sido sobre los riesgos que tienen estos dispositivos y que controles y auditoría necesitan estos dispositivos.

Este último post he decidido dedicarlo a introducir algunos riesgos más, en función del área al que pertenece, puesto que comenté que me parecía un tema interesante en mi post relacionado con los riesgos. Si bien es cierto, que algunos riesgos se repetirán, pienso que es importante categorizarlos.

Riesgos

A continuación, planteo un pequeño esquema que resume los riesgos de cada área y acto seguido explicaré detalladamente cada una de estas [1].

- Área financiera
    - Salud y seguridad
    - Cumplimiento normativo
    - Privacidad del usuario
    - Costos inesperados
- Área operacional
    - Acceso inadecuado
    - Uso en la sombra
    - Rendimiento
- Área técnica
    - Vulnerabilidad del dispositivo

- Actualizaciones del dispositivo
- Administración del dispositivo

Área financiera

El riesgo más grave que puede ocurrir en esta área es en el impacto en la salud y la seguridad si se modifica el funcionamiento de un dispositivo. Varias investigaciones han demostrado que se pueden realizar ataques a dispositivos biomédicos como un marcapaso o un desfibrilador. A su vez, también se pueden realizar ataques contra los coches, pudiendo deshabilitar el sistema de frenos cuando este está en marcha.

Además, como bien expliqué en mi post relacionado a los riesgos se puede obtener todo tipo de información de los dispositivos IoT. Si bien los dispositivos cuentan con medidas de seguridad como una contraseña, esta es opcional. Esto hace que la US Federal Trade Commision haya demandado algunas empresas por políticas de seguridad pobres.

También, los riesgos regulatorios son posibles, especialmente en los dispositivos embebidos. Los riesgos regulatorios ocurren principalmente cuando se está procesando información sensible, cuando se interactúa con procesos regulados por los gobiernos y por el impacto que tienen en sistemas críticos. Los dispositivos que procesan personales pueden estar tratando con información privada o sensible del usuario, lo cual implica un riesgo a la privacidad del usuario.

Finalmente, los costos inesperados suelen surgir cuando un se cambia un dispositivo no informático por uno que si lo es. Esto es debido a que el dispositivo informático requiera conectividad o soporte adicional para realizar la tarea completa.

Área operacional

Además de los riesgos financieros que implica utilizar un

sistema embebido, hay que tener en cuenta otros riesgos. Uno de estos riesgos es contar con una comunicación M2M insegura. Esto hace que personal inapropiado pueda realizar cambios en el dispositivo u obtener telemetría de este.

También, la implementación de dispositivos sin una supervisión centralizada ni una gobernanza adecuada puede ser perjudicial para los dispositivos IoT. Este tipo de implementación se llama Shadow IT. Al no contar con nadie que se encargue de que los dispositivos estén protegidos, esto puede hacer asumir riesgos adicionales a la empresa la empresa.

Riesgos técnicos

Los dispositivos IoT embebidos suelen ser más complejos de configurara que los dispositivos tradicionales, causado por el gran número de dispositivos IoT. Estos dispositivos, al igual que los dispositivos tradicionales pueden ser atacados como bien mencioné en mi post sobre riesgos.

Los ataques realizados contra los dispositivos IoT ofrecen un desafío para los fabricantes, debido a que muchas veces la única manera de corregir la vulnerabilidad es actualizar el hardware.

Finalmente, desde el punto de vista de la administración de estos dispositivos, muchas empresas no están preparadas para poder proporcionar la seguridad necesaria a estos dispositivos. Esto hace que deban considerar cuestiones como la realización de inventarios, la supervisión de acceso al dispositivo etc. al igual que en los sistemas tradicionales.

Conclusión final

Mientras buscaba información para realizar estos artículos he descubierto un sinfín de características que desconocía sobre los dispositivos IoT. A su vez, como he ido comentando a lo largo de varios artículos, el número de dispositivos IoT ha

estado creciendo durante los últimos años y se espera que siga creciendo en los próximos años. Además, creo que esta tecnología está revolucionando todos los sectores de la industria y que va a seguir incluyendo muchas mejoras. Finalmente, me gustaría recordar que estos dispositivos tienen un gran número de riesgos, los cuales creo que irán decreciendo en los próximos años.

Bibliografía

[1] <<Internet of Things: Risk and Value Considerations>>, ISACA, consultado el 20/11/2020, https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpiot