Controlando nuestro alrededor

Como ya hablé en el post anterior, IoT es capaz de poner en riesgo partes muy importantes de nuestras organizaciones o vidas privadas. Es por esto, que las empresas, ya sean grandes, medianas o pequeñas, deben hacer el ejercicio de revisar los sistemas que tienen implantados para detectar los riesgos que pueden llegar a tener, de esta manera, podrán implementar un sistema de controles que les permita mitigar el daño que dichos riesgos puedan llegar a causar. Es en este punto en el que el trabajo del auditor se convierte en vital.

Lo primero que debe hacer la compañía al implantar nuevos sistemas que incluyan dispositivos de IoT es revisarlos de manera que se puedan identificar los riesgos que se van a añadir a la organización y posteriormente implantar un plan de migración de los mismos para minimizar los daños. Entre medias de este proceso entra en juego el papel de la auditoria de seguridad. En esta, los auditores deberán identificar los riesgos que existan y crear unos controles para revisar y mitigar dichos riesgos.

Es en este momento cuando los auditores pueden crear un cuadro de controles a aplicar. En este cuadro se listan los riesgos que se han detectado y los controles que se pueden aplicar a estos. En estos cuadros también se pueden añadir los ámbitos de impacto de dicho riesgo, los responsables de realizar los controles o los puestos/empleados a los que puede afectar de ocurrir. A continuación, tenemos un cuadro en el que se han listado unos de los riesgos más críticos en IoT y los controles que se pueden aplicar: [1]

Riesgo	Control
Ataques físicos al dispositivo	• ¿Es el dispositivo accesible físicamente a cualquier persona? • ¿Está el dispositivo vigilado? • ¿Está el dispositivo monitorizado contra alteraciones hardware?
Manipulación de datos en el dispositivo	• ¿Está el dispositivo cifrado? • ¿Cuenta el dispositivo con un código de autenticación de mensajes o firma digital?
Ataques de interceptación (Man-in-the-middle)	• ¿Está el dispositivo protegido a nivel de protocolo? • ¿Está el dispositivo emparejado?
Manipulación del sistema operativo	• ¿Está el sistema operativo en modo lectura solo? • ¿Está el sistema operativo firmado? • ¿Está el sistema operativo cifrado?
Acceso no autorizado al dispositivo	• ¿Tiene contraseña el dispositivo? ¿Es segura? • ¿Qué puertos están abiertos?
Accesos de terceros	• ¿Tiene el dispositivo programas de terceros instalados? ¿Son seguros? • ¿Tenemos contacto con los desarrolladores de los programas instalados?

Una vez realizada esta tabla la organización será la encargada de asegurarse que dichos controles se van realizando periódicamente y que se reporta si se encuentra alguna anomalía. También tendrá que preparar a los responsables de llevarlos a cabo de manera que sepan realizarlos correctamente.

En este ámbito nos podemos encontrar con frameworks que usan tecnologías muy innovadoras, como blockchain, que prometen crear un sistema de fiabilidad para los dispositivos IoT. En el reto que es crear este framework, se proponen solucionar el problema que existe a la hora de gestionar el acceso a los dispositivos. El framework propone una solución para crear un sistema que conceda y revoque el acceso a los dispositivos mediante una blockchain descentralizada, anónima y segura. Dicho framework, que esta recién sacada del laboratorio, es la prueba de que el campo de IoT está en auge y que se

están utilizando tecnologías muy innovadoras para tratar de crear nuevos sistemas que permitan controlar y hacer más seguros nuestros dispositivos más personales. [2]

Por otra parte, también existen «frameworks» o guías más experimentadas que nos brindan buenos consejos para la compra, implantación e instalación de dispositivos IoT en nuestras empresas, como es el caso de OWASP IoT Project. Mediante este proyecto se quiere ayudar a los fabricantes, desarrolladores y compradores de IoT a prestar atención a los problemas de seguridad más importantes que presentan los dispositivos y como se pueden mitigar o controlar. [3]

El rol del auditor en todo este proceso es vital ya que él o ella será el encargado de crear un sistema preventivo para que la organización a la que ha auditado no tenga ningún problema o sea capaz de controlarlos. Es por esto por lo que los auditores tienen una gran responsabilidad dentro de la empresa ya que su juicio es vital para impedir que ocurran problemas que le cuesten grandes cantidades de dinero a las organizaciones.

Referencias:

[1] <<Cyber risk in an Internet of Things world>>, Deloitte, acceso el 27 de Noviembre de 2017, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html#

[2]<<Internet of Things: Risk and value considerations>>, LinkedIn, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

[3]<<Fairaccess>>, LinkedIn, acceso el 27 de Noviembre de 2017, https://es.slideshare.net/mimolik/fairaccess

<<FairAccess: a new Blockchain-based access control framework for the Internet of Things>>, Oscars Laboratory, acceso el 27 de Noviembre de 2017, http://download.xuebalib.com/xuebalib.com.31639.pdf

<<Internet of Things: Risk and value considerations>>, Isaca, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

<<OWASP Internet of Things Project>>, OWASP, acceso el 27 de Noviembre de 2017, http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf