Controles y auditoria para los sistemas de control industrial

En el anterior post estudiamos los riesgos que afectan a los sistemas de control industrial. Pudimos ver que el mayor problema que rodea a los sistemas de control industrial es su tecnología anticuada y por lo tanto que estos resultan vulnerables a ataques, es decir van atrasados en materia de ciberseguridad. Esto se debe a que en un principio fueron diseñados para usarse en lugares que no estuviesen expuestos a una red externa, sin embargo los tiempos cambian y han obligado a estos sistemas a estar conectados tanto con otros sistemas de la empresa como con la red global debido a la cuarta revolución industrial.

Hay muchos desafíos que enfrentan la protección de sistemas de control industrial, que van desde técnicas, tales como protocolos de comunicación débiles (en su mayoría sin cifrar) o la larga vida útil de estos sistemas, a organizativos (por ejemplo, la falta de colaboración y coordinación entre los departamentos involucrados) y gubernamentales, por ejemplo la falta de una política de seguridad en operadores de infraestructura crítica.

Un problema muy importante que ha sido incluido entre los ocho mayores desafíos en la seguridad de sistemas de control industrial es que los miembros de alta dirección de las empresas que utilizan sistemas de control industrial no están suficientemente involucrados en la seguridad del sistema de control industrial [1].

Comenzaremos identificando los controles necesarios teniendo en cuenta los riesgos estudiados anteriormente. Debido a que el riesgo que identificamos hace referencia a la ciberseguridad y esta está estrechamente relacionada con la seguridad de la información tomaremos como referencia el estándar ISO 27002. Sin embargo solo haremos uso de aquellos controles que tengan que ver con nuestro tema, que son los siguientes:

RIESGO	NIVEL DE RIESGO	CONTROL

Conexión remota a los sistemas	Alto	6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 12.4.1 Registro y gestión de eventos de actividad.
Integración con otros sistemas TI de la empresa	Alto	5.1.2 Revisión de las políticas para la seguridad de la información. 12.3.1 Copias de seguridad de la información. 12.7.1 Controles de auditoría de los sistemas de información.

Uso de dispositivos portátiles	Medio	8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 12.3.1 Copias de seguridad de la información.
Falta de renovación de la tecnología	Alto	12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.7 Externalización del desarrollo de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.

Falta de concienciación y comunicación sobre la seguridad	Alto	6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.4 Contacto con grupos de interés especial. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad.
Inadecuada gestión del cambio	Medio	12.1.2 Gestión de cambios. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software.

Conexión con una red global	Alto	9.4.1 Restricción del acceso a la información. 10.1.1 Política de uso de los controles criptográficos. 11.1.6 Áreas de acceso público, carga y descarga. 12.2.1 Controles contra el código malicioso. 13.1.1 Controles de red. 13.2.1 Políticas y procedimientos de intercambio de información. _ 14.1.3 Protección de las transacciones por redes telemáticas.

Como podemos observar los riesgos relacionados los sistemas de control industrial están altamente relacionados con la seguridad de la información, con la conexión de estos sistemas a la red los datos quedan expuestos a atacantes en la red o incluso que se encuentran dentro de la empresa. Por ese motivo utilizando todos los controles mencionados anteriormente somos capaces de controlar y mitigar los riesgos [2].

En pocas palabras me gustaría mencionar que los controles para asegurar la información de los sistemas de control industrial son totalmente necesarios. Por ese motivo las empresas deberían tenerlas muy en cuenta a la hora de implantar estos sistemas o incluso renovarlos. La auditoría sobre los sistemas de control industrial es más que necesaria para la adecuación de estos sistemas a las nuevas demandas de la industria, además de asegurar su continuidad mientras la empresa siga realizando sus labores dentro del sector en el que esta se desenvuelve.

Referencias:

[1] Deusto Océano. <<Approaching secure industrial control systems>>.Acceso 27 de noviembre de 2018. https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_scopus2-s2.0-84918570350&context=PC&vid=deusto&lang=en_US&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,industri

al%20control%20systems&sortby=rank&offset=0

[2] ISO27000.<<ISO27002>>. Acceso 27 de noviembre de 2018. http://www.iso27001security.com/html/27000.html

---

Network Connected Devices (Internet of Things): Riesgos (parte 2, Final)

Mitigación y Priorización

En este apartado se analizará y se profundizará más en cada uno de los riesgos descritos en la subsecciones anteriores, finalizando con una tabla que contendrá un resumen con el impacto del riesgo y su probabilidad.

Salud y Seguridad

Los riesgos de salud y seguridad están relacionados estrechamente con el negocio. El impacto en todos los casos es alto, dado que involucra vidas humanas o repercute en el medio ambiente. La probabilidad de que se dé depende del negocio en cuestión y de las funciones de las que se encargue el dispositivo IoT.

Este riesgo está sensiblemente relacionado al resto de los riesgos de negocio, operacionales y técnicos ya que cualquiera de estos puede comprometer tanto a la salud como a la seguridad.

Para mitigar este riesgo es necesario realizar un modelo holístico para prevenir, detectar y corregir las posibles vulnerabilidades del dispositivo. Este modelo consiste en identificar a los *Stakeholders* para poder definir el ámbito de uso. Una vez definido esto, se realiza una evaluación de los riesgos para identificar las posibles vulnerabilidades y determinar el impacto de negocio que supondría que ocurrieran dichos riesgos. A continuación, es necesario desarrollar un plan de contingencia que garantice la seguridad y el buen funcionamiento del dispositivo. Por último, y no menos importante, se requiere realizar un proceso de monitorización continua para salvaguardar y/u obtener evidencias de que todo va según lo establecido y realizando siempre un análisis actualizado de las posibles vulnerabilidades que pudieran comprometer la seguridad del dispositivo.

Cumplimiento de la regulación

Los riesgos de cumplimiento de regulación dependen del país en el que resida la sede de la organización y de la legislación de los países en los que ofrezca servicio.

Una organización se enfrenta a estos riesgos, mayormente, cuando se producen

cambios en la ley o la regulación que afectan a la industria o un negocio, que pueden implicar cambios en los procesos, *frameworks* y costes. Dependiendo del negocio, estos cambios pueden suponer el cierre del mismo por lo que supone un impacto alto, aunque, con una buena gestión, es dificil que esto ocurra por lo que la probabilidad resultante es media.

Para mitigar los posibles riesgos referentes al cumplimiento de la regulación es necesario hacer una gestión de la misma. Ésta casi siempre va de la mano de una auditoría, ya sea externa o interna, en la que se definirá qué rasgos de la regulación afectan más a la empresa. Con esto, se exigirán las evidencias que demuestran que se cumple con la regulación para asegurarse que todo funciona como lo exige la ley. Este proceso requerirá realizar una monitorización periódica para controlar los posibles cambios jurídicos que puedan surgir.

Privacidad del usuario

La privacidad del usuario está ligada a las vulnerabilidades del dispositivo, leyes de los países en los que se opere y de cómo la organización gestione los datos de carácter personal. Teniendo en cuenta que más del 90% de dispositivos contiene información sensible y de que de éstos el 70% presenta algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta. El impacto representa una sanción económica por parte del órgano judicial, así como una pérdida de confianza de los usuarios, por lo que supone que el impacto sea alto.

Para mitigar estos riesgos, por una parte el usuario ha de estar concienciado y entender lo que suponen los siguientes factores del IoT:

- La interoperatividad entre dispositivos y tecnologías.
- Como la información se transmite entre dispositivos y aplicaciones.
- Los términos “privacidad” y “condiciones de uso” de los dispositivos.
- El riesgo de compartir información entre los dispositivos y las redes sociales.
- La implicación de vincular cuentas presentes en las redes sociales.

Conociendo estos factores el usuario entenderá cuales son sus derechos y se pensará dos veces qué tipo de contenido comparte en la red.

Por otra parte, la organización debe cumplir según la regulación de los países en los que opere. Se establecerán las responsabilidades de las organizaciones externas que tengan acceso a dicha información y se llevarán a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Costes inesperados

El hacer uso de esta nueva tecnología supone una implantación y un desarrollo más lento. Por otra parte, un cambio en los estándares exigiría una nueva planificación, modificación de fechas de entregas y una inversión de fondos adicionales. De todas formas, haciendo un análisis de los riesgos, no serán tan arriesgados como para poner en peligro la organización. Es por ello que

la probabilidad de este riesgo es media y el impacto es bajo.

En estos casos, es aconsejable seguir las novedades que realizan los organismos responsables del estándar para poder planificar de antemano cualquier imprevisto y asignar un margen de costes para solventar o mitigar dichos imprevistos.

Acceso inadecuado

Una vulnerabilidad en el dispositivo, puede implicar un acceso inadecuado al mismo. Por otra parte, con la reducción de coste de los dispositivos, cada vez son más los que se sitúan en áreas desprotegidas exponiendo, físicamente, la integridad del sistema. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente disposición de dispositivos sin monitorización, la probabilidad de acceso inadecuado es alta, siendo su impacto alto dado a que pueden afectar tanto a la salud y seguridad como a la privacidad de la información del usuario.

Para mitigar este riesgo, es necesario restringir el acceso al dispositivo, bien físicamente o mediante un sistema de autenticación y autorización lo suficientemente robusto. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Uso inapropiado

Las vulnerabilidades del dispositivo implican que usuarios no autorizados puedan acceder a los procesos de los dispositivos y alterar su funcionamiento. Por otra parte, los usuarios, como tal, pueden utilizar el dispositivo o componentes del mismo con fines para los que no fueron diseñados. En el primer caso el riesgo es alto, dado que pueden comprometer la salud, la seguridad y la privacidad de los datos. Debido al alto número de dispositivos que presentan vulnerabilidades y a la creciente existencia de los mismos, sin monitorización, la probabilidad de que se dé un uso inadecuado del dispositivo es alta.

Para mitigar este riesgo, sobre el uso inadecuado por parte del usuario, es necesario definir una política de uso que exhuma de responsabilidad a la organización de su uso indebido. Por otra parte, será necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Rendimiento

El rendimiento se puede ver alterado por un uso inapropiado de los recursos causado por una vulnerabilidad del dispositivo o por un mal diseño, esta última siendo menos probable. Dependiendo de la funcionalidad que desempeñe el dispositivo, el impacto variará. Como ejemplo, no es lo mismo un sistema de monitorización de aviones que el sensor que monitoriza la temperatura de la calefacción de una vivienda, es por ello que el impacto puede ser alto o bajo. En lo que respecta a su probabilidad, debido al alto número de dispositivos que presentan vulnerabilidades, la probabilidad de una

alteración del rendimiento es alta.

Para mitigar este riesgo, es necesario realizar un modelo holístico para descubrir las posibles vulnerabilidades del diseño del dispositivo así como cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos.

Vulnerabilidades del dispositivo

Superar este reto es sin lugar a dudas uno de los retos más duros a los que se enfrenta el IoT dado a la diversidad de vulnerabilidades que se han encontrado en los dispositivos ya existentes en el mercado. Se calcula que cerca del 70% de los dispositivos IoT presentan algún tipo de vulnerabilidad, entre las que cabe destacar:

- El 80% de estos dispositivos tiene una contraseña débil o corta o políticas de seguridad insuficientemente complejas.
- El 70% de los dispositivos falló a la hora de encriptar los servicios de transmisión de datos por la red local e Internet.
- El 60% de los dispositivos con interfaz web permiten realizar ataques de *cross-site scripting*, mantienen las credenciales por defecto o realizaban una mala gestión de la sesión.
- Por otra parte, al no haber un estándar universal definido, seguido de unas buenas prácticas del desarrollo para comunicación entre dispositivos, muchos de ellos realizan conexiones inalámbricas de protocolos que presentan vulnerabilidades, como los que se pueden mostrar en la parte inferior de la figura 2.

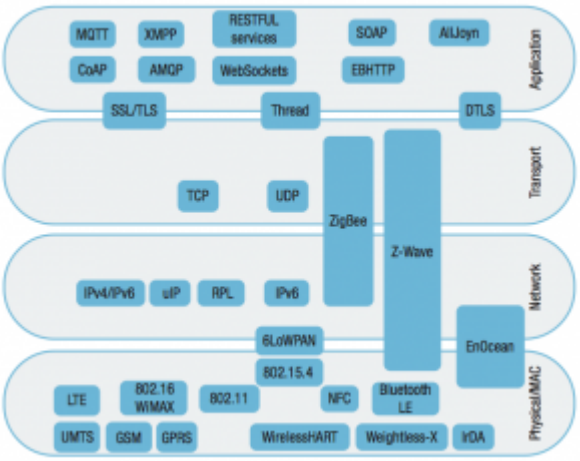

Figura 2: Protocolos más usados en el IoT

Como se deduce, la probabilidad de que un dispositivo presente vulnerabilidades de algún tipo es alta. Por otra parte, tal y como se ha visto en las subsecciones anteriores, este riesgo compromete aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que supone también es alto.

Para mitigar algunos de estos riesgos es necesario realizar las siguientes tareas:

- Desarrollar una legislación, políticas, estandares y buenas prácticas.
- Liberar el software propietario no compatible a la comunidad *open-source*.
- Asegurarse de que los sistemas embebidos remotos están monitorizados o su vida útil es finita.
- Integrar la seguridad en los procesos de diseño de los dispositivos.
- Realizar un estudios de los servicios que se utilizan para la comunicación y puedan crear situaciones inseguras o no deseadas y planear una arquitectura para salvaguardarse de estas vulnerabilidades.
- Definir y habilitar comprobadores de la integridad de los datos en los dispositivos.

Actualizaciones del dispositivo

Este riesgo consiste en no mantener al dispositivo y brindarle actualizaciones que solventen vulnerabilidades. Pero además, incluye las vulnerabilidades propias de dicho proceso:

- La comunicación entre el servidor y el cliente no está cifrada, pudiendo así acceder al contenido del mismo.
- Los clientes que no protegen el espacio de memoria destinado a la actualización, siendo posible la instalación de un código de terceros.

Al igual que los riesgos de seguridad, estos riegos comprometen aspectos tan críticos como la salud, seguridad y la privacidad del usuario, por lo que el impacto que suponen es alto. Por otra parte, debido al alto número de dispositivos vulnerables, la probabilidad de padecer este riesgo también es alto.

Mitigar este riesgo consiste en impedir que los usuarios consigan aprovecharse de las vulnerabilidades de dispositivos no soportados o no actualizados y asegurar los procesos de actualización. Para ello hay que llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como definir un ciclo de vida para los dispositivos, monitorizados y darlos de baja cuando llegue el momento.

Gestión del dispositivo

Este riesgo consiste en salvaguardar los procesos de configuración, supervisión y mantenimiento de los dispositivos, donde entran en juego las vulnerabilidades y el acceso autorizado. Una mala monitorización o la configuración por un usuario no autorizado puede comprometer la salud, seguridad y la privacidad de la información, por lo que el impacto de este riesgo es alto. Por otra parte, debido a la gran cantidad de dispositivos que presentan algún tipo de vulnerabilidad, la probabilidad de este riesgo es alta.

Para mitigar este riesgo, es necesario llevar a cabo las medidas de seguridad enumeradas en los apartados relacionados a los riesgos técnicos, así como establecer un control sobre los usuarios que están autorizados para la manipulación del dispositivo sin olvidarnos de una continua monitorización.

Riego	Impacto	Probabilidad
Salud y seguridad	Alto	Bajo-Alto (Dependiente de Negocio)
Cumplimiento de la regulación	Alto	Bajo
Privacidad del usuario	Alto	Alto
Costes inesperados	Medio	Bajo
Acceso inadecuado	Alto	Alto
Uso inapropiado	Alto	Alto
Rendimiento	Bajo-Alto (Dependiente de la función que desempeña el dispositivo)	Alto
Vulnerabilidades del dispositivo	Alto	Alto
Actualizaciones del dispositivo	Alto	Alto
Gestión del dispositivo	Alto	Alto

Priorización de los riesgos

Seguridad en la Nube. ¿Cómo mitigar los riesgos?

Me gustaría empezar con la definición de la computación en la nube según el Instituto Nacional de Estándares y Tecnología: » La computación en nube es un modelo para permitir a conveniencia, acceso a la red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente suministrados y liberados con un esfuerzo de gestión o interacción con el proveedor de servicios mínimo». Otras organizaciones adoptan un enfoque más simple y definen la computación en nube como servidores virtuales disponibles

en Internet. Independientemente de la definición, la computación en la nube es un fenómeno que sigue creciendo en popularidad en el mundo de los negocios.

Considero que las ventajas de la computación en nube son innegables. La tecnología cloud ofrece una mayor flexibilidad, permitiendo a los usuarios disfrutar de una mayor movilidad, proporciona a las organizaciones un mayor almacenamiento y reduce la carga de los departamentos de TI que utilizan sistemas informáticos convencionales. Son estas necesidades y la conveniencia de subcontratar estos requisitos lo que sigue marcando el creciente uso de la computación en nube. Sin embargo, ninguna tecnología está libre de posibles complicaciones. Como las organizaciones están recurriendo cada vez más a la computación en la nube, los riesgos asociados con el uso de esta son cada vez más claros, de los cuales el más importante es la seguridad.

Los riesgos asociados con el uso de la computación en la nube dependen de varios factores tales como el tipo de actividad, la cantidad de datos en la subcontratación y el proveedor de servicio seleccionado. Sin embargo, siempre que se utilizan soluciones cloud el seguir estas estrategias permite mitigar el riesgo en cuanto a la seguridad:

- **Investigar y analizar las soluciones cloud:** Cuando tu empresa pretende migrar parte de su hardware y software a la nube, necesitas informarte sobre los potenciales proveedores. Esto incluye examinar el historial de seguridad del proveedor, la comprobación de referencias, la comprobación de vulnerabilidades de seguridad conocidas, y asegurarse de que el contrato con ellos incluye prácticas de seguridad proactivas por su parte.
- **Utilizar una solución Single Sign-on(SSO) para añadir seguridad:** Dependiendo del tamaño de la organización, se podría dar el caso de estar creando muchas cuentas de usuario para diferentes servicios en la nube. Un usuario puede tener varias cuentas y contraseñas, lo que hace que sea más complicado para el usuario y el administrador. Reduciéndolo a un entorno de inicio de sesión único, se reduce el número de posibles debilidades de seguridad.
- **Trabajar con un tercero para asegurar seguridad en la nube de forma regular**: Por lo general, tener múltiples proveedores aumenta los riesgos de seguridad y las pequeñas y medianas empresas sin grandes departamentos de TI a veces necesitan ayuda para auditar y garantizar la seguridad en la nube. Es importante contratar las auditorias de terceros para asegurarse de que su proveedor de la nube está siguiendo las normas de seguridad.
- **Implementar el cifrado end-to-end:** El cifrado end-to-end, en particular para el almacenamiento en la nube, disminuye la probabilidad de que sus datos sean violados. La mayoría de las soluciones de almacenamiento en la nube han cifrado la carga y descarga de datos, pero no el almacenamiento. El método con menos riesgo requiere que sus datos sean encriptados antes de subir, mientras están almacenados por el proveedor, y que sólo se puedan descifrar con una clave de cifrado única.
- **Actualizar regularmente su software:** No hay que descuidar el software cuando se migre a la nube. Si se están ejecutando sistemas operativos

obsoletos como Windows XP y navegadores obsoletos como IE 7, se podría estar en riesgo a pesar del cifrado y las auditorias de terceros.