Gestión de un inventario de activos en Sistemas de Control Industrial

Durante los últimos años hemos sido testigos de cómo los sistemas de control industrial (SCI) también son susceptibles de sufrir un incidente de ciberseguridad. Cada vez es mayor la concienciación, y cada vez más organizaciones implementan medidas de seguridad para conseguir elevar el nivel de ciberseguridad de sus dispositivos y redes Sin embargo, sigue habiendo un problema recurrente: el desconocimiento del total de activos por parte de las organizaciones y su respectivo alcance.

Si no se conoce el alcance total difícilmente vamos a poder tomar medidas para asegurar todos nuestros dispositivos, quedando algunos desprotegidos. Siguiendo el principio de que una cadena es tan fuerte como su eslabón más débil, podemos concluir que, si no aseguramos todos los activos por igual, estas medidas son insuficientes.

Las numerosas ventajas son:

- Facilidad a la hora de gestionar vulnerabilidades de los sistemas, ya que, en todo momento, tendremos identificadas las versiones presentes en los mismos.

- Una respuesta a incidentes más eficiente y estructurada, ya que, al conocer todos los activos implicados en el proceso es más fácil determinar el alcance del incidente y agilizar la subsanación del mismo.

- Identificación de fallos a nivel operativo. Un inventario de activos no solo proporciona ventajas a nivel de ciberseguridad, sino que también permite mejorar los procesos para hacerlos cada vez más eficientes.

- Reducción de costos, debido a la mejora de la seguridad y conocimiento de todos los activos.

La realización de un inventario de activos debería ser uno de los primeros pasos a ejecutar en la implementación de un plan para la gestión de la

ciberseguridad en sistemas de control industrial, con el objetivo de asegurar los elementos que los componen, y de esta manera poder descubrir elementos de los que no se tenía conocimiento.

Existen diferentes formas y soluciones que permiten el desarrollo de un inventario de activos. Entre las más comunes se encuentra el uso de hojas Excel, que permiten almacenar información de cada activo identificado y modificar sus datos en cualquier momento; el uso de bases de datos con una interfaz gráfica, ya sea de escritorio o web, para comodidad de uso por parte de los usuarios responsables, etc.

Estas soluciones guardan algunas características comunes, como pueden ser la facilidad de uso y de acceso o la posibilidad de exportar la información para ser tratada posteriormente, obteniendo inteligencia derivada de la información procesada.

Un inventario automático se elabora gracias al uso de herramientas que permiten agilizar las tareas de recopilación de datos de cada activo de manera automática, algo especialmente útil cuando el número de activos de una organización es muy elevado.

Un posible problema que puede darse en el uso de estas herramientas es la falta de información deseable sobre cada uno de los activos, que podría ser insuficiente, puesto que las herramientas podrían no facilitar todo el material necesario de cada activo, debido a que no se ha recopilado o no se ha conseguido toda la información que se necesita de él.

Un inventariado realizado de forma pasiva es aquel que no realiza ninguna acción de manera directa sobre los activos para obtener información sobre los mismos y, por lo tanto, no es tan intrusiva como la forma activa. Este tipo de inventariado nos permite conocer cierta información sobre los activos, no siempre de manera precisa, pero sin provocar algún impacto sobre los mismos. Dentro de los inventariados ejecutados de manera pasiva podemos encontrar el inventariado realizado a través de un análisis de tráfico o el análisis de los ficheros de configuración de los activos. Un inventariado pasivo realizado de manera mixta sería el análisis de red, ya que se utilizan herramientas automáticas pero cierta información se analiza de manera manual; mientras que el análisis de los ficheros de configuración sería un ejemplo análisis pasivo manual.

Hardware		Todos los equipos físicos empleados en el desarrollo del proceso industrial.	PLC RTU IED Servidores
Software		Aplicaciones utilizadas para la gestión del proceso.	SCADA Sistemas operativos Sistemas de desarrollo
Personal		Personal que trabaje en la organización.	Fijos Subcontratados
Información		Datos que se generan, recogen, gestionan, trasmiten y destruyen, independiente de su formato.	Bases de datos Documentación Manuales
Red		Los dispositivos de conectividad de red.	Routers Switches Cortafuegos
Tecnología		Equipos necesarios para gestionar las personas y el negocio de la empresa.	Ordenadores Teléfonos Impresoras Cableado
Equipamiento auxiliar		Activos que no se encuentran en ninguna de las categorías anteriores y que dan soporte al resto de sistemas.	Climatización Iluminación
Instalaciones		Lugares en los que se alojan los equipos relevantes de la empresa.	Oficinas Edificios

Se tendrá que definir el alcance del inventario, el cual no hace referencia a la cantidad de activos a incluir, que deberán ser todos, sino al tipo de profundidad en la información a recopilar de cada uno de ellos. Esto supondrá que se revise exhaustivamente el alcance de los dispositivos, incluyendo, si fuese necesario, varios inventarios; o clasificarlos en distintos grupos debido a la cantidad y tipos diferentes que se puedan tener a la hora de gestionarlos. La necesidad de un buen inventario de activos a la hora de realizar proyectos de ciberseguridad es un factor clave que ayudará a la realización de un buen trabajo. Además, al definir un alcance correcto de la información de los activos que se van a incluir, se podrán proteger de una manera más eficiente a la hora de gestionar sus vulnerabilidades.

NOZOMI NETWORKS

Descubrimiento de activos de forma automática

- Rastrea automáticamente sus activos de OT e IT. Permitiendo localizar rápidamente equipos dentro de la red y alertando de accesos no autorizados.
- Identifica las caracteristicas principales de cada activo, como hostname, ip, Firmware, fabricante, entre otras.
- Mantiene un inventario actualizado.
- Clasifica la infraestructura por niveles de acuerdo con el modelo de Purdue

Fuente: INCIBE