Inventario de activos

El inventario de activos conforma el primer elemento de la cadena en un sistema de gestión de la seguridad de un sistema. Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Para proteger adecuadamente los sistemas de control industrial, las organizaciones ya no pueden confiar estrictamente en enfoques tradicionales basados en TI o el sistema físico para la gestión de activos de ciberseguridad. Las amenazas evolucionan continuamente y los ataques a infraestructuras críticas y sistemas de control industrial son cada vez más sofisticados y frecuentes.

- Funciones esenciales para la mejora de la seguridad -

Es habitual encontrar un inventario de activos incompleto o inexistente en entornos de sistemas de control, lo que constituye uno de los grandes inconvenientes a la hora de abordar otras mejoras de la seguridad de estos sistemas. No se puede proteger lo que no se conoce, por eso es muy importante disponer de un inventario de activos convenientemente actualizado y revisado.

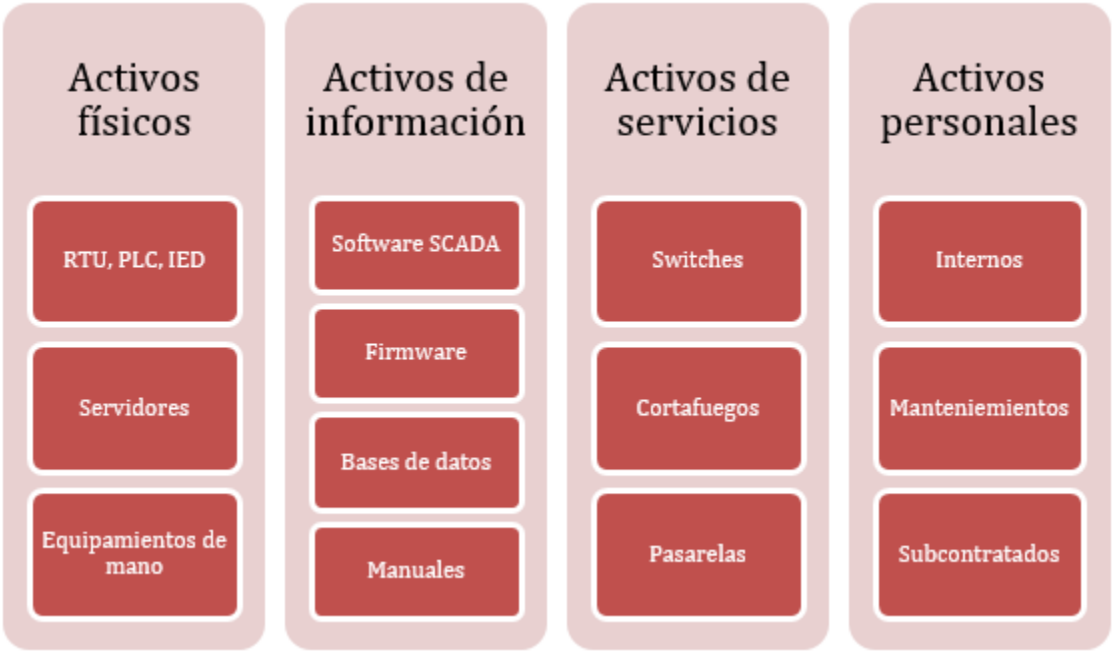
Clasificación de activos en el inventario

La información que se recoge en un inventario de activos varía dependiendo del alcance del mismo. Es recomendable que exista un equipo de seguridad encargado de su gestión y actualización, así como de su revisión anual y tras cada incorporación o eliminación de activos. Este equipo será responsable de tareas como definir, inventariar y categorizar los diferentes activos dentro de los sistemas de control, así como de las redes internas y externas, según el alcance del inventario.

El inventario debe tener un enfoque global que abarque todos los sistemas dentro de su alcance y debe incluir tanto PLC, DCS, SCADA, así como los elementos de supervisión como HMI y otros dispositivos y sistemas auxiliares.

Para facilitar el manejo y mantenimiento del inventario, es conveniente clasificar los activos por categorías, según su naturaleza:

- ***Datos:*** Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen. Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.).
- ***Aplicaciones:*** El software que se utiliza para la gestión del proceso. Sistemas SCADA, herramientas de desarrollo de HMI, aplicativos desarrollados, sistemas operativos, firmware de dispositivos, etc.
- ***Hardware industrial:*** Equipos físicos necesarios para desarrollar la labor industrial (terminales remotas, PLC, IED, PC, servidores, dispositivos móviles o de mano, etc.)
- ***Red:*** Dispositivos de conectividad de redes (routers, switches, concentradores, pasarelas, etc.)
- ***Tecnología:*** Otros equipos necesarios para gestionar las personas y el negocio de la empresa (servidores, equipos de usuario, teléfonos, impresoras, routers, cableado, etc.).
- ***Personal:*** En esta categoría se encuentra tanto la plantilla propia de la organización como el personal subcontratado, personal de mantenimiento y, en general, todos aquellos que tengan acceso de una manera u otra a la industria.
- ***Instalaciones:*** Lugares en los que se alojan los sistemas relevantes del sistema (oficinas, edificios, instalaciones eléctricas, vehículos, etc.).
- ***Equipamiento auxiliar:*** En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, SAI, etc.).



- Ejemplo de clasificación de activos -

Información de cada activo

Para que pueda aportar valor en la evaluación de la seguridad y en la gestión de riesgos, un inventario de activos tiene que proveer información suficiente para futuros proyectos o incidentes, así como proporcionar una visión precisa de los valores de los mismos de forma que sea posible establecer los criterios la realización de un análisis de riesgos.

Para ello debe recoger la información relevante de cada sistema como podría ser:

- ***Nombre:*** Puede incluir modelo, marca, nombre descriptivo, etc.
- ***Descripción:*** No es necesario que sea demasiado extensa, pero sí debe contener información sobre el uso del activo.
- ***Identificador:*** Código único para el activo. Debe seguir un patrón elegido por la empresa
- ***Tipo:*** Recoge el grupo al que pertenece el activo.
- ***Propietario:*** Todo activo debe tener un propietario. Este será el encargado de tomar decisiones como el reemplazo del mismo.
- ***Responsable:*** El responsable es la persona encargada de que el activo se encuentre operativo, así como de gestionar los accesos al mismo. En muchas ocasiones podrá coincidir con el propietario.
- ***Ubicación:*** Lugar donde se encuentra físicamente el activo. Si se trata de un activo físico la ubicación será un lugar, si se trata de un activo lógico la ubicación será un activo físico.
- ***Valoración del activo:*** Valor a asignar al activo que permita evaluar su impacto en el sistema. Para ello pueden tenerse en cuenta diversos parámetros como por ejemplo:
    - ***Disponibilidad:*** Valor cualitativo o cuantitativo que determine la importancia que tiene la ausencia del activo.
    - ***Integridad:*** Valor cualitativo o cuantitativo que determine las repercusiones para el negocio que tendría la modificación del activo sin autorización.
    - ***Confidencialidad:*** Valor cualitativo o cuantitativo que determine el grado de confidencialidad que requiere el activo.
    - ***Criticidad:*** Valor que determina la dependencia del proceso con el activo. A mayor valor de criticidad mayores consecuencias para el negocio supone la pérdida del activo.
    - ***Coste:*** Valor económico del activo.

Gestión eficiente del inventario de activos

Mantener actualizado el inventario de activos puede ser una tarea muy costosa si se realiza de forma manual por diferentes causas:

- Tiempo invertido en su elaboración
- Desconocimiento de componentes o instalaciones
- Falta de permisos adecuados para acceder a los activos incluidos en el inventario.

Además, es una tarea propensa a errores humanos. Los datos recogidos, a menudo están incompletos y esto va empeorando la calidad del inventario con el tiempo.

Existen en el mercado herramientas del mundo TI dedicadas al inventariado de activos que facilitan la tarea de identificar y documentar todo el hardware y software residente en una red. Sin embargo, para la utilización de este tipo de herramientas es necesario conocer correctamente su funcionamiento y el impacto que podrían tener en los equipo de control conectados a la red. Es recomendable realizar una evaluación previa de la herramienta en entornos fuera de producción para garantizar que su funcionamiento no altera el sistema a inventariar. El impacto en el sistema al utilizar estas herramientas, podría ser debido a la naturaleza de la información o al volumen de tráfico de red que, si bien puede ser aceptable en los sistemas de TI, no tiene por qué serlo en los sistemas de TO.

La gestión automatizada permite disponer de forma más precisa y eficiente del inventario de activos y es, sin lugar a dudas, una herramienta a tener en cuenta tanto por razones de seguridad como por su capacidad de retorno de la inversión al permitir un sustancial ahorro en los costes relacionados con la gestión de incidentes.

Fuente: https://www.incibe-cert.es/blog/inventario-activos