Configuraciones seguras

Regulaciones como la CRA (Cyber Reisilience Act), la nueva NIS2 o el hecho de prestar servicios a las administraciones públicas están promoviendo la cultura de la ciberseguridad dentro de las organizaciones. La adopción de estándares como ISO27001, ISA/IEC62443 o el ENS están obligando a las organizaciones a desarrollar y adoptar una política de seguridad dentro de la organización.

Las políticas proporcionan el marco general de seguridad, establecen las directrices y responsabilidades, mientras que los procedimientos operativos se encargan de la ejecución práctica de esas políticas. Uno de los procedimientos básicos que hay que desarrollar es el de securización de los sistemas dentro de la organización.

Definimos la securización como la implementación de medidas de seguridad que protejan al sistema de potenciales ataques y vulnerabilidades. Al securizar los sistemas las organizaciones están reduciendo el riesgo de accesos no autorizados, filtraciones de datos u otros incidentes de seguridad.

Existen una serie de estrategias generales para la securización de los sistemas entre las que se pueden citar: gestión de parches, configuración segura, control de accesos, supervisión y registro, encriptación y repuesta a los incidentes. Nos centraremos en este artículo en la configuración segura de los dispositivos.

Existen diferentes componentes que tenemos que tener en cuenta para configurar de manera segura un dispositivo.

- **Inventario de activos**

  Lo que no se conoce no se puede proteger. Mantener actualizado el inventario de los dispositivos que están en el sistema y disponer no solo del número de los dispositivos sino también su configuración, versiones de hardware, firmware o software, posición física y conexiones lógicas con otros dispositivos. El inventario es un elemento vivo que hay que ir actualizando de manera periódica con nuevos dispositivos o con los cambios que se hayan producido en los elementos ya existentes.

- **Gestión de los servicios y los puertos**

  Deshabilitar los servicios y los puertos que no sean necesarios. Habilitar únicamente los servicios que se vayan a usar y utilizar siempre las versiones seguras de los servicios. La idea es reducir la superficie de ataque y limitar potenciales puntos de entrada de los atacantes. Se reduce el riesgo de accesos no autorizados.

⇨ **Contraseñas**

Cambiar las contraseñas por defecto y requerir el uso de contraseñas fuertes con un número suficiente y variado de caracteres o, dependiendo del dispositivo, requerir el cambio regular de las contraseñas o mejor aún el uso de autenticación multifactor. Se reduce el riesgo de accesos no autorizados

⇨ **Gestión de las cuentas de usuario**

Crear varias cuentas en función de los requisitos de cada rol y asegurarse de implementar contraseñas distintas. Seguir siempre el principio de mínimo privilegio y permitir a los usuarios solo los permisos necesarios para realizar su función y ninguno más. De esta manera reducimos el riesgo de accesos no autorizados, limitamos el impacto de las amenazas internas y mantenemos la confidencialidad.

⇨ **Gestión de firmware/software**

Mantenerse informado de los últimos parches de seguridad de los fabricantes disponibles para los dispositivos y mantener todos los dispositivos actualizados a la ultima versión disponible. Aunque no todas las organizaciones son iguales y debe existir un procedimiento de parcheo donde se recojan cuales son los pasos para aplicar el parcheo en los diferentes dispositivos, los riesgos del parcheo, necesidad de un banco de pruebas, responsables...

Como hemos visto la configuración segura juega un papel importante en fortalecer la postura de seguridad de los sistemas, mitigando riesgos y mejorando la resiliencia frente a las ciber amenazas. Al implementar de manera eficiente las practicas de configuración segura las organizaciones pueden crear entornos seguros que protegen datos sensibles, mantienen la continuidad de la operación y cumplen con los requerimientos regulatorios.

Juan Manuel Herrera

Ingeniero ciberseguridad OT

Elecnor