Ciberseguridad:
PUNTO DE ACCESO SEGURO

PROCETRADI

Las **subestaciones eléctricas** son consideradas como infraestructura crítica debido a su importancia en el suministro del servicio eléctrico. Por ello, es necesario contemplar los lineamientos básicos de seguridad física y virtual para el acceso a ellas. Dentro de estos lineamientos podemos encontrar todo aquello relacionado a puntos de accesos seguro (PAS).

Entendamos un **punto de acceso** como una puerta virtual en la subestación que permite la entrada y salida de información. De esta forma, un punto de acceso seguro se entiende como las puertas o interfaces que permiten tener un control del ingreso o salida de los datos intercambiados entre una subestación y sistemas externos.

Un **PAS** necesita contemplar como mínimo dos funcionalidades:

1) Es un punto conocido y fácilmente identificable.

2) Permite limitar el acceso de cualquier ente externo no deseado a una subestación.

El concepto de punto seguro a una subestación ya se encuentra normado en estándares internacionalmente usados como la **NERC-CIP**, el cual podemos encontrar el capítulo 005, donde se detalla que todas las comunicaciones desde y hacia una subestación necesitan pasar por un punto de acceso seguro identificado (Identified Electronic Access Point).

¿Qué consideraciones debe tener un punto de acceso ***PARA SER CONSIDERADO SEGURO?***

Se debe contemplar:

a) Toda comunicación necesita ser *ruteable*:

En una subestación es usual encontrar un mínimo de dos segmentos. El primer segmento es el segmento de **comunicación**, el cual se encarga de enlazar la subestación con sistemas externos como SCADA o ingeniería y mantenimiento. El segundo segmento está relacionado a la **comunicación interna** en una subestación, comprendiendo el intercambio de información entre los equipamientos control, medición y protecciones.

Para entender la importancia de este proceso, imaginemos la data de una subestación como un edificio corporativo. Si el edificio no posee paredes, cualquier ente externo podría tomar la información contenida. Para evitarlo, se coloca una puerta que canalice cualquier salida o entrada de información, con ello no solo se tiene un control de la información que se intercambia, sino que también permite limitar el acceso de agentes externos a la **información crítica** de operación.

b) Se debe de limitar el número de segmentos o direcciones IP con permisos de acceso:

Regresando al ejemplo, si bien la puerta principal permite tener un control del ingreso, no garantiza la restricción del acceso a las áreas o habitaciones del edificio. Para esto, se tienen los módulos de recepción donde se valida que la persona tenga los permisos de entrada y guía en dirección al área final. De igual forma, el uso de segmentos diferenciados no garantiza que agentes externos no entren a aplicaciones que no tengan autorización.

Para prevenir esto, se recomienda el uso de **reglas de tráfico** de llegada y salida de paquetes. Estas reglas, usualmente configuradas mediante un firewall, permiten seleccionar los segmentos y/o direcciones IP con accesos a ciertas aplicaciones y funcionalidades en la subestación. Esto agrega un mayor grado de protección ya que, además de restringir a nivel de segmentos, también se restringe a nivel de aplicación o puerto TCP.

c) Uso de encriptación o protocolos seguros para la comunicación externa a una subestación:

El uso de encriptación o protocolos seguros en una subestación permite el resguardo de la información desde la fuente de intercambio **(IEDs o RTUs)**. Esto nos permite resguardar la información contenida en este intercambio de paquetes. Puedes encontrar más información de tipos de encriptación y protocolos seguros en nuestro artículo "Ciberseguridad: encriptación en las comunicaciones de una infraestructura eléctrica".

d) Implementación de credenciales de acceso y perfiles de usuario:

El uso de usuarios y perfiles de usuario permite la restricción a la configuración, monitoreo y control del equipamiento en una subestación, limitando la operación únicamente al personal que posee las credenciales con los perfiles respectivos. Esta medida también facilita rastrear cualquier cambio y/u operación en las unidades a los usuarios registrados en el sistema.

La gestión de la **autenticación** en una subestación se puede desarrollar de forma centralizada y distribuida. La primera concentra toda la base de datos de usuarios en un servidor central, el cual sincroniza a clientes sobre el estado de los usuarios. El segundo, maneja una base de datos local e independiente en cada uno de los equipos.

¿Por qué es necesario contemplar estos ***LINEAMIENTOS EN UNA SUBESTACIÓN?***

Gracias al desarrollo tecnológico que nos permite tener **infraestructura eléctrica remota** 100% desatendidas, las subestaciones de hoy se caracterizan por poseer varios subsistemas funcionando en paralelo. Es durante la operación de estos subsistemas y su conectividad con distintos segmentos externos de la subestación, que se expone el contenido de operación a múltiples segmentos y usuarios. Esto agrega un factor de riesgo a que cualquier información crítica pueda ser interceptada o extraída, incrementando el riesgo y probabilidad de un ciber ataque a la infraestructura eléctrica.

Si deseas tener más información de cómo implementar un punto de acceso seguro en tu **infraestructura eléctrica**, escríbenos a marketing@procetradi.com

PROCETRADI

www.procetradi.com