Ciberseguridad:

ENCRIPTACIÓN EN LAS COMUNICACIONES DE UNA INFRAESTRUCTURA ELÉCTRICA

PROCETRADI

Con la llegada de la tecnología digital y la masificación de los servicios remotos que obligan la utilización de redes públicas, las **empresas eléctricas** necesitan contemplar lineamientos de seguridad para la protección de su data operativa en la red. Una de las tecnologías más utilizadas es la **encriptación de las comunicaciones**.

Para entender el concepto, imaginemos la **data operativa** como artículos u objetos que viajan dentro de un camión. La carretera que comunica los puntos A y B representa el **canal de comunicación en la red**, mientras que el camión que transporta los objetos equivale al **protocolo TCP** elegido para la transferencia de información. Al igual que en las comunicaciones en redes públicas, la carretera por donde transita el camión puede ser accedida por cualquier agente. De esta forma, se puede interceptar el vehículo y extraer los objetos o artículos dentro de este. Por lo tanto, entendamos **encriptación** como los mecanismos que vamos a usar para evitar que agentes no autorizados tomen posesión de la información durante el traslado.

En la actualidad existen distintos tipos de encriptación, sin embargo, las más utilizadas en la **industria eléctrica** las podemos agrupar en 3:

1) **Redes privadas virtuales o VPNS**

2) **Encriptación de trazas mediante TLS**

3) **Uso de protocolos con autenticación segura**

¿Qué son VPNs?

Imaginemos que el camión transita por la misma carretera, pero que se "crea" un carril dedicado exclusivamente para el tránsito de los camiones que salen del punto A y B. Si alguien durante el trayecto desea entrar, no le es permitido debido a que es una **"ruta privada"** dentro de una carretera pública, y para ingresar necesita pasar los controles necesarios de identificación.

Por lo tanto, **VPN** consiste en la utilización de una **red privada virtual** dentro de una red pública. Para ello se utilizan túneles virtuales que encriptan toda la información a transmitirse entre los servidores, ya que generan un enlace privado dentro de la red pública.

El uso de esta tecnología se encuentra masificado debido a su robustez y amplio soporte por distintos desarrolladores. Sin embargo, debido a la tecnología involucrada, su uso en la industria eléctrica suele estar más relacionada a las áreas de tecnologías de la información (TI) de las empresas. Por ello, las áreas operativas de las empresas eléctricas necesitan el soporte del área de TI para la implementación, administración y mantenimiento de estas redes.

¿Qué es la encriptación MEDIANTE TLS?

Imaginemos ahora que los artículos u objetos del camión, son divididos en pequeñas partes y desorganizados como si fuese una rompecabeza de 10,000 piezas. Si un agente externo logra interceptar el camión y extrae el artículo, estos no van a poder armar el rompecabezas e identificar el contenido si no poseen información de cómo armar el rompecabezas. Por ello, para cualquier agente externo que no posea el patrón de las piezas individuales o una imagen referencial, el contenido representa muchas piezas sueltas sin sentido.

Por lo tanto, **encriptación mediante TLS** significa descomponer el contenido a trasmitir y reorganizarlo de tal manera que para su interpretación necesites el ***patrón o llave*** con el cual fue creado. Este proceso conocido como encriptación requiere que las *llaves o patrones* para la interpretación, sean compartidos por ambos extremos de la comunicación.

El uso de esta tecnología simplifica el uso de equipamiento especializado, debido a que los servidores únicamente necesitan tener un administrador de llaves de encriptación para su implementación. Sin embargo, necesita contemplar conocimiento de redes para su adecuada configuración, mantenimiento y gestión.

¿Qué son los protocolos ***CON AUTENTICACIÓN SEGURA?***

Imaginemos ahora que el camión viaja con un candado o cerrojo, que únicamente necesita de la autenticación del emisor y receptor para poder ser abierto. De esta manera, si un agente externo no identificado intenta abrir el candado, el sistema no permitirá su apertura ya que no se encuentra dentro de la lista de usuarios permitidos. Además, cada intento fallido de acceso al candado queda registrado y es compartido entre los participantes de la comunicación, con el propósito de tener **métricas de seguridad** de la comunicación.

Por lo tanto, la **autenticación segura** significa crear una identificación del emisor y receptor, además de entregar métricas de intentos fallidos de acceso o paquetes perdidos, entre otros. Los más usados en la industria eléctrica son tecnologías desarrolladas en los mismos protocolos de comunicación. De esta forma, se tiene el **Secure Autentication (SA)** del protocolo **DNP3**, el cual se encuentra en su versión 6 actualizada el año 2020 (v5 la más comercial), o el **Secure Autentication** basado en el **estándar IEC60870-5-7** para el protocolo **IEC608750-5-104**.

Debido a que la aplicación de esta tecnología se encuentra más asociada al **protocolo eléctrico**, su uso simplifica la necesidad del soporte especializado, relevando la responsabilidad del uso, gestión y mantenimiento al área operativa.

Es importante detallar que cada una de las tecnologías descritas no son restrictivas entre sí, sino que se complementan para cubrir todos los requerimientos en las comunicaciones de una **subestación**. De esta forma, es usual encontrar el uso de **VPNs** para la comunicación entre el centro de control y subestaciones, así como el uso de **encriptación con TLS** para comunicación entre equipamiento crítico de la subestación con equipamiento en campo como reconectadores. Finalmente, se suele utilizar **Secure Autentication** para la comunicación con IEDs dentro de la misma subestación eléctrica.

Si deseas tener más información de como implementar encriptación en tu **infraestructura eléctrica**, no dudes en comunicarte con nosotros escribiendo a **marketing@procetradi.com**.

www.procetradi.com