CÓMO FRUSTRAR A LOS HACKERS

Detección de intrusión en redes con supervisión funcional

de Yann Gosteli, Centralschweizerische Kraftwerke AG

Un concepto de seguridad eficaz para las subestaciones no solo contempla el control de acceso físico y los cortafuegos, sino que también supervisa lo que está ocurriendo en la red de la estación. Dado que los ciberataques pueden causar importantes problemas de suministro de energía, la compañía eléctrica suiza Centralschweizerische Kraftwerke AG (CKW) ha implementado una serie de medidas diseñadas para mejorar la seguridad de sus futuras subestaciones.

La infraestructura que soporta el suministro de energía es crítica, por lo que se está convirtiendo en un objetivo cada vez más atractivo para los ciberataques. Si los hackers son capaces de tomar el control silencioso de una subestación o de partes de sus equipos, las consecuencias para el funcionamiento de la red y el suministro de cantones enteros en Suiza son potencialmente muy graves y pueden incluso afectar a la infraestructura esencial. Esto exige medidas eficaces de ciberseguridad no solo en el centro de control de la red, sino también en la propia subestación.

Normas de calidad suizas

Por lo tanto, en CKW hemos estado prestando mucha atención al tema de la seguridad en la tecnología de automatización, control y protección de las subestaciones. Durante la fase de planificación del nuevo concepto de subestación, hemos hecho mucho hincapié en mantener un alto nivel de ciberseguridad. Se implementará por primera vez cuando la nueva subestación de Rothenburg entre en funcionamiento en 2020.

Como somos muy conscientes de nuestra responsabilidad en este aspecto, CKW es también miembro del grupo VSE (Verband Schweizerischer Elektrizitätsunternehmen [Asociación de compañías eléctricas suizas]), que publicó el «Handbuch Grundschutz für ‹Operational Technology› in der Stromversorgung» [Manual de protección básica de la tecnología operativa en el suministro de electricidad]. Estamos continuamente integrando los resultados y las ideas que se derivan de este esfuerzo en nuestros propios proyectos, incluido el concepto de subestación de 2020. Este manual ha sido elaborado pensando en todo el sector. Describe un método de defensa en profundidad para proteger las redes tecnológicas operativas. Analiza a fondo todos los aspectos de la seguridad de los datos, la información y las operaciones. Esto incluye crear e implementar conceptos de zonificación, monitorearlos, y detectar y responder ante determinados eventos de seguridad. Como compañía eléctrica, el monitoreo y la detección deben permitirnos minimizar el impacto de un ataque en el sitio.

Seguridad por diseño

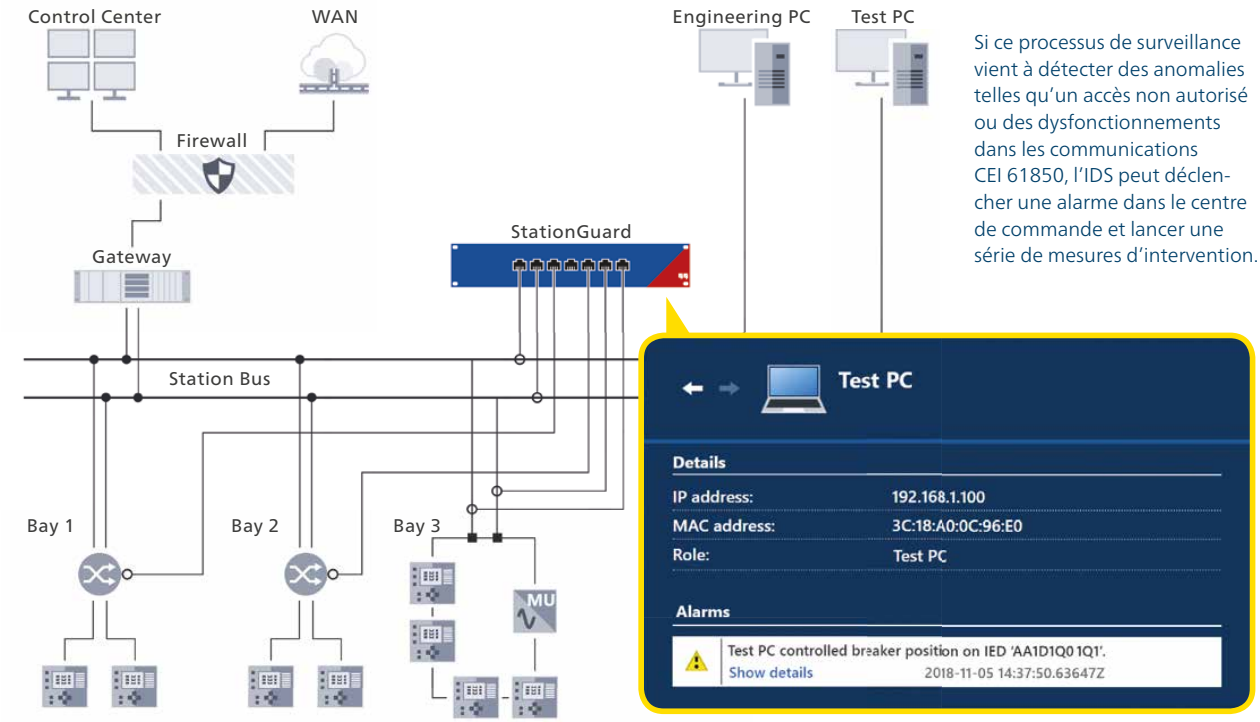
El método que seguimos para diseñar la red de la subestación de Rothenburg fue el de poner en marcha una serie de capas de defensa para separar zonas individuales y hacer más difícil el ataque a la red de procesos. Para ello hemos tenido en cuenta toda una serie de aspectos de seguridad: Las conexiones IP de la subestación al mundo exterior se desactivan durante las operaciones normales; las conexiones de acceso remoto solo se habilitan bajo demanda; todo el acceso a los componentes

con fines de servicio técnico se realiza exclusivamente mediante estaciones de trabajo centralizadas especiales que se han reforzado adecuadamente. Este tipo de acceso se habilita de forma remota solo cuando se solicita. Todos los demás clientes conectados a la red también se refuerzan, por ejemplo, mediante el bloqueo de funciones innecesarias del sistema operativo basados en el perfil de usuario.

Ejecutamos el sistema SCADA, el sistema de recopilación de registros de perturbaciones y los servicios de seguridad virtualizados en un servidor de la subestación. El control de todos los derechos de acceso a estos sistemas se gestiona de forma dedicada. Esto significa que cada estación de trabajo local solo puede acceder a los sistemas utilizando conexiones de escritorio remotas y un cortafuegos local. Los usuarios tienen que iniciar sesión en estas estaciones de trabajo mediante un Directorio Activo (AD) central, que les asigna los derechos y permisos necesarios. Además, los usuarios tienen que iniciar sesión en cada uno de los IED del sistema de automatización de la subestación mediante sus contraseñas personales, tras lo cual se les conceden los derechos correspondientes desde el servidor de control de acceso a través de Radius. Esto se aplica tanto al acceso a los dispositivos con herramientas de ingeniería como al control en la pantalla del IED. No se utilizan contraseñas estándar.

*«StationGuard es realmente fácil de usar. Se me **presenta toda la información que necesito en un formato claro y familiar,** sin ningún tipo de jerga informática».*

Yann Gosteli,
Head of Substation Automation Systems, Centralschweizerische Kraftwerke AG



Si ce processus de surveillance vient à détecter des anomalies telles qu'un accès non autorisé ou des dysfonctionnements dans les communications CEI 61850, l'IDS peut déclencher une alarme dans le centre de commande et lancer une série de mesures d'intervention.

Las redes de proceso y de servicio técnico están separados lógica y físicamente. Las comunicaciones utilizando el protocolo IEC 61850 Ed. 2 se implementan en una interfaz diferente de la utilizada para acceder a los dispositivos con fines de ingeniería o mantenimiento. Toda la red de procesos está segmentada y cada segmento está separado de los demás por un cortafuegos redundante.

Decidimos utilizar un diodo de datos para manejar la transferencia de datos desde la instalación a los niveles superiores de la red. Un diodo de datos garantiza que ningún tráfico de red externo pueda acceder a la instalación.

Monitoreo frente a hackers dentro de la instalación

Todas estas medidas por sí solas proporcionan un alto grado de seguridad, pero no pueden evitar un ciberataque con un 100 % de certeza. Para prever esta eventualidad, buscamos un sistema de monitoreo que reconozca todo comportamiento no conforme en la red e inmediatamente emita una alarma. El sistema de detección de intrusión StationGuard (IDS) de OMICRON era la solución perfecta para nuestras necesidades. Este IDS ha sido desarrollado específicamente para su uso en subestaciones y está compuesto por una solución de software que funciona sobre un sistema operativo especialmente robusta y una plataforma de hardware igualmente robusta llamada RBX1, que podemos instalar directamente en la subestación gracias a sus dimensiones compatibles con el bastidor.

StationGuard lee automáticamente el contenido del archivo SCL (lenguaje de configuración de la subestación) específico del sitio y genera un modelo del sistema, que luego compara continuamente con los eventos de la subestación. Si este proceso de monitoreo detectara alguna anomalía, tales como accesos no autorizados o mal funcionamiento en las comunicaciones IEC 61850, el IDS puede emitir una alarma en el centro de control e iniciar una serie de acciones de respuesta. Todos los eventos y alarmas se visualizan gráficamente de una forma que resulta familiar tanto para los ingenieros de control y protección como para los especialistas informáticos. Para evitar falsas alarmas durante las actividades de mantenimiento, el ingeniero informará con antelación al IDS sobre el equipo de prueba que se utilizará y cambiará StationGuard al modo de mantenimiento para esa sesión.

Con sus amplias funciones de monitoreo y unos requisitos mínimos de configuración y servicio técnico, StationGuard nos proporciona un aumento significativo de la seguridad de las subestaciones.