INDUSTRIA

AUTORIDAD DEL AGUA DE UN ÁREA URBANA

OPTIMIZAR LA SEGURIDAD TENIENDO EN CUENTA LAS RESTRICCIONES OPERATIVAS

1,3 millones
DE HABITANTES

60
MUNICIPIOS

100
TORRES DE AGUA

Redes cada vez más inter-conectadas

La seguridad de las instalaciones de agua es un problema importante para las zonas urbanas. El intercambio de información se hace permanente entre las redes informáticas y operativas. Sin embargo, esta optimización de la gestión de las infraestructuras aumenta la superficie de ataque. Por ejemplo, en marzo de 2016, un hacker atacó una planta de agua potable de Estados Unidos. Los malhechores habían alterado la cantidad de productos químicos en el agua. Más recientemente, en abril de 2020, el gobierno israelí hizo pública una serie de ciberataques a sus instalaciones de suministro y tratamiento de agua. La agencia de ciberseguridad de Israel ha dado instrucciones a todo el personal de las empresas que operan en los sectores de la energía y el agua para que cambien las contraseñas de todos los sistemas conectados a Internet.

El contexto

El principal centro urbano, con unos sesenta municipios y más de un millón de habitantes, de una gran región francesa, ha lanzado una licitación para racionalizar la gestión de su red de agua potable. Durante varios años, esta distribución de agua había sido gestionada por tres operadores privados de distribución. El objetivo es ahora tener un solo operador. Además de esta racionalización del servicio, la ciudad también quería modernizar su arquitectura informática aumentando el nivel de seguridad.

Los tres operadores existentes se encontraron entonces en competencia para gestionar el servicio público de producción, transporte, almacenamiento y distribución de agua potable en la mayor parte de la zona.

Además, para reforzar la seguridad de sus redes operativas, la ciudad quería una arquitectura que permitiera una protección independiente mediante la implantación de cortafuegos para:

- la red del departamento de TI,
- los concentradores VPN centrales,
- los sistemas de información industriales y de seguridad,
- las ubicaciones remotas.

La solución elegida

Esta licitación fue ganada por el operador líder en el mercado francés, que recurrió a Stormshield para que le ayudara a proteger este entorno industrial.

Las principales funcionalidades previstas y habilitadas en esta arquitectura global son el control y el filtrado de cada comunicación con DPI (principalmente el protocolo Modbus), así como la implementación de una solución VPN IPsec para proteger las comunicaciones

Fuertes restricciones industriales gestionadas a través de una única solución

La seguridad de la sede central se ha reforzado con la instalación de cortafuegos entre la red de la oficina y las instalaciones empresariales. Estas instalaciones se encuentran en dos redes distintas (de seguridad e industrial), cada una de ellas protegida por un conjunto de cortafuegos diseñados para actuar como concentradores VPN. Esta arquitectura interconecta estas mismas aplicaciones a las distintas torres de agua.

En concreto, el operador eligió un clúster de cortafuegos SN3100 para proteger la red operativa y de seguridad y evitar cualquier interrupción gracias a la doble fuente de alimentación y los discos RAID integrados en estos equipos.

También se desplegaron tres clústeres de cortafuegos SN710 para la zona del concentrador VPN (comunicación IT/OT). Gracias a los informes interactivos personalizables, el cliente tiene acceso instantáneo a la información esencial sobre la actividad de la red y los eventos relacionados con la seguridad. El sistema de protección contra intrusiones (IPS) se basa en varios métodos de detección de comportamientos y está directamente integrado en el núcleo de los productos, proporcionando una protección eficaz contra las amenazas de día cero y manteniendo un rendimiento de alta velocidad.

Por último, 100 torres de agua han sido equipadas individualmente con dos clústeres (uno para la seguridad y el segundo para la parte industrial) con cortafuegos reforzados SNi40 para proteger los flujos entre las diferentes ubicaciones y aplicaciones. Están diseñados específicamente para proteger los PLC (controladores lógicos programables) y también permiten túneles VPN IPsec hacia los sitios centrales.

La oferta industrial propuesta por Stormshield respondía perfectamente a las distintas necesidades expresadas por el operador. Además, la adaptabilidad de la solución propuesta permitía gestionar tanto los sitios estándar como los entornos con grandes restricciones industriales (temperatura, humedad, carril DIN, fuente de alimentación industrial). Todo ello, con el mismo firmware desplegado en toda la gama Stormshield Network Security y una única consola de gestión, Stormshield Management Center, para gestionar toda la flota de cortafuegos.

Además, más allá de la relación funcionalidad/precio e independientemente de las funciones estándar (VPN, segmentación, etc.), el cliente se sintió muy atraído por la funcionalidad IPS para los protocolos industriales, con la granularidad más avanzada del mercado y que permite que la seguridad de estos sistemas sensibles evolucione a medida que se modernizan las infraestructuras.

Una gama de servicios adaptados a entornos industriales complejos

En lo que respecta al mantenimiento y la operación, el cliente se enfrentaba a problemas de accesibilidad y sensibilidad de determinados emplazamientos para garantizar la disponibilidad del servicio a los usuarios. Para superar estas limitaciones, Stormshield y el operador seleccionado han implementado un sistema de soporte adaptado, con:

- La implementación de un procedimiento que permite a un agente técnico sin conocimientos de redes/seguridad sustituir un cortafuegos que falla y hacer que el sitio vuelva a funcionar con el nivel de seguridad adecuado,
- Una activación del modo de seguridad (bypass) para el 5% de los sitios que no están equipados con un clúster sino con un solo cortafuegos. Se trata de priorizar la disponibilidad y la seguridad de los sistemas industriales sobre la seguridad,
- Una serie de servicios profesionales para apoyar al área local en su proceso de despliegue de la configuración de los sitios piloto iniciales.

El conjunto del proyecto y su puesta en marcha fue un éxito y se realizó a tiempo de principio a fin gracias a la fuerte implicación y cohesión entre el operador y el fabricante El cliente final también valoró muy positivamente la aplicación de los procedimientos para responder a las necesidades del negocio en este entorno industrial.

Y la relación continúa, ya que Stormshield ha llevado a cabo otros proyectos y ha respondido a licitaciones junto a este operador, que también se pone en contacto internamente para modernizar su actividad y ajustar su oferta a este entorno de seguridad IT/OT. Ya que esta cuestión es cada vez más vital cuando se trata de infraestructuras sensibles y críticas cuyos riesgos cibernéticos podrían tener graves consecuencias económicas, medioambientales y humanas.

STORMSHIELD

En todo el mundo, empresas, instituciones gubernamentales y organizaciones de defensa necesitan garantizar la seguridad digital de sus infraestructuras críticas, datos sensibles y entornos operativos. Las tecnologías de Stormshield, certificadas y calificadas al más alto nivel europeo, responden a los retos de las TI y las OT para proteger sus actividades. Nuestra misión: dar a nuestros clientes tranquilidad en cuanto a los riesgos cibernéticos para que puedan concentrarse en su actividad principal, tan crucial para el buen funcionamiento de nuestras instituciones, nuestra economía y los servicios prestados a la población. Elegir Stormshield es optar por una ciberseguridad europea de confianza. Más información: www.stormshield.com