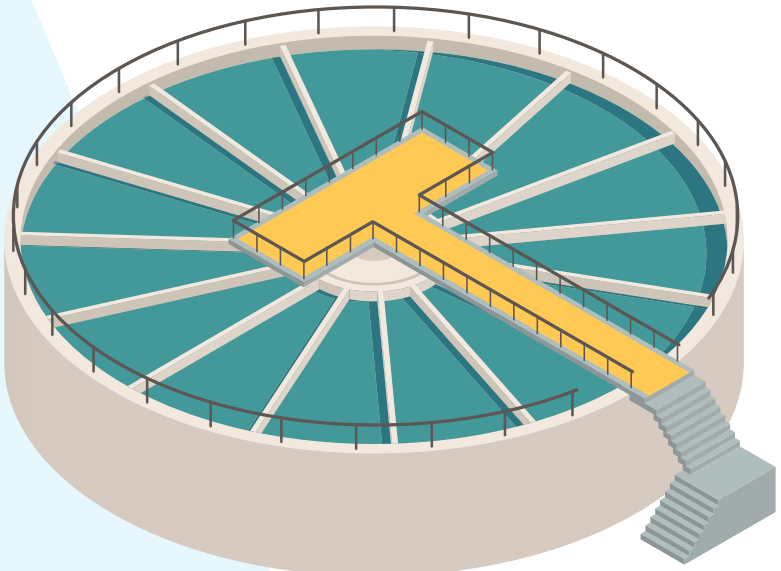
STORMSHIELD

La Ciberseguridad
en entornos sensibles:

Inmersión en el sector del agua

Libro blanco



Tres días...

Esa es la esperanza de vida de un ser humano privado de agua. De ahí la importancia vital de este recurso.



Pero el agua también es necesaria para las actividades agrícolas e industriales y para la comodidad de los hogares. ¿Durante cuánto tiempo podrían las empresas seguir funcionando con normalidad después de cerrar el grifo, especialmente en un mundo afectado por el calentamiento global?

El trabajo de los actores del sector del agua – comunidades y empresas privadas en servicio público delegado – es garantizar que nunca tengamos que descubrirlo. Tienen una doble responsabilidad ante las personas y el medio ambiente. En primer lugar, deben dar continuidad a la producción y distribución de agua potable, garantizando al mismo tiempo la seguridad sanitaria. En segundo lugar, es su responsabilidad tratar las aguas residuales, para evitar su contaminación cuando se vierten al medio natural o se reutilizan.

En Francia, por ejemplo, el sector es lo suficientemente sensible como para ser coordinado por el Ministerio responsable de la Ecología y supervisado diariamente por un coordinador sectorial de la agencia de ciberseguridad ANSSI.

Sin embargo, este denso ecosistema industrial, formado por plantas de producción de agua potable o de tratamiento de aguas residuales – algunas de las cuales están clasificadas como "operadores de servicios esenciales" a nivel europeo – se apoya en infraestructuras y tecnologías envejecidas que lo hacen vulnerable. Además, estos sistemas de explotación están ahora mucho más expuestos al riesgo cibernético porque, como consecuencia de la digitalización del sector y la llegada de nuevas tecnologías, se encuentran cada vez más conectados a las redes informáticas.

Este fenómeno de convergencia IT/OT se ilustra con la implementación de Ethernet IP incluso en las fábricas, y también con el desarrollo de soluciones en la nube para la supervisión industrial. Se trata de una superficie de ataque atractiva para los ciberatacantes, que suelen dominar más las tecnologías informáticas tradicionales que los protocolos industriales específicos.

Además, ya sea en Estados Unidos o en Israel, los casos de ciberataques contra empresas de agua se han multiplicado en los últimos años. Y en todo el mundo, las empresas e instituciones públicas vinculadas al sector del agua se van concienciando

de la necesidad de garantizar la seguridad digital de sus infraestructuras críticas, datos sensibles y entornos operativos.

Este aumento del riesgo cibernético también pone de manifiesto la fragilidad de un sector que ha sufrido una falta de inversión. En Europa, al igual que en Estados Unidos, las infraestructuras de agua son gestionadas en su mayoría por pequeñas organizaciones y generan bajos márgenes.

Sus sistemas industriales se amortizan mucho menos que una red de oficinas y suelen estar equipados con PLC de antigua generación, lo que aumenta su vulnerabilidad. Y como la inversión en equipos informáticos repercute directamente en el precio del litro de agua, estas organizaciones también deben afrontar la necesidad de controlar los costes, para mantener el acceso del público en general.

Debido a la insuficiencia de recursos y a la inmadurez en este ámbito, los gestores de las redes de agua han priorizado durante mucho tiempo la protección de la salud pública sobre la protección de sus sistemas de información.—

El objetivo de este libro blanco es, por tanto, permitir a los responsables de TI, y a todo el ecosistema de subcontratistas (integradores y fabricantes) del sector, sumergirse en un examen de la cuestión de la ciberseguridad en el sector del agua.

En las siguientes páginas, le ofreceremos explicaciones sobre los problemas de este sector y le proporcionaremos un inventario operativo de posibles soluciones.

Contenidos

Cifras a recordar

• **Infografía —** Cartografía del mundo del agua

PARTE I.

¿Por qué el sector del agua debería tomar en serio las cuestiones sobre ciberseguridad?

PARTE II.

¿Un futuro de (ciber) guerras del agua?

• **Entrevista 1 a un cliente —** Punto de vista: la ciberseguridad, un hábito que el sector del agua está aprendiendo a adquirir

PARTE III.

¿Cuáles son los cuestiones que impulsan la ciberseguridad en el sector del agua?

• **Infografía —** Las principales vulnerabilidades en el sector

PARTE IV.

¿Qué ciber regulaciones existen en el sector del agua?

PARTE V.

¿Y qué pasará mañana?

• **Entrevista 2 a un cliente —** Proteger una red distribuida

Cifras
a recordar

33.200

estructuras de captación de agua estudiadas en Francia (FP2E, 2019). Para evitar que se contaminen, las leyes de aguas de 1992 y 2006 prevén tres perímetros de protección de las captaciones (inmediato, cercano, lejano) y un mecanismo para evitar la contaminación difusa en las zonas de abastecimiento de estas captaciones. En ese momento no se menciona la ciberseguridad.

40 a 45%

Este es el **índice de fugas** en las redes de distribución de agua de las ciudades de Nueva York, Londres y Roma (frente a una media del 20 al 25% en el resto del mundo, según Les Échos Investir, 2021). El objetivo es evitar estas brechas mediante la gestión remota y el mantenimiento predictivo.

400

El número de habitantes de Chatsworth (norte de Georgia, EE.UU.) que no pudieron utilizar el agua del grifo durante varios días en 2013. El motivo: una intrusión en el sistema de vigilancia de una instalación de agua potable de la ciudad y cambios en los ajustes de los niveles de flúor y cloro.

46

El número de intentos infructuosos de penetrar en los sistemas de información de una planta de tratamiento de aguas residuales en Australia en el año 2000. Desgraciadamente, al 47º intento, el antiguo proveedor de servicios técnicos de la fábrica consiguió hacerse con el control de la misma, vertiendo las aguas residuales al fondo del mar.

3

El número de crisis cibernéticas relacionadas con el agua que ha sufrido sólo Israel en el año 2020. Entre abril y diciembre, los ciberataques afectaron a estaciones de bombeo y tratamiento de agua, a bombas de agua y a un depósito de agua reciclada.

Más de 3 de cada 5 vulnerabilidades

en los sistemas de información industrial pueden provocar la indisponibilidad total de la herramienta de producción si se explotan eficazmente. Y el 72% de ellas pueden ser explotadas de forma remota. *(Claroty, 2020).*

52%

de la población mundial vivirá en condiciones de estrés hídrico en 2050 (Naciones Unidas, 2019) – lo que acentúa aún más las cuestiones ya estratégicas relacionadas con este recurso.

x2

Los sistemas operacionales de la industria del agua tienen más del doble de vulnerabilidades que el sector sanitario, aunque estuviera especialmente expuesto durante la crisis sanitaria.*(Claroty, 2020).*

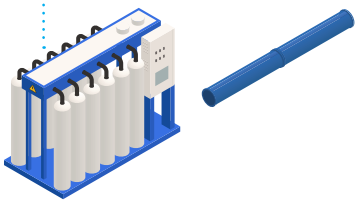
Infografía

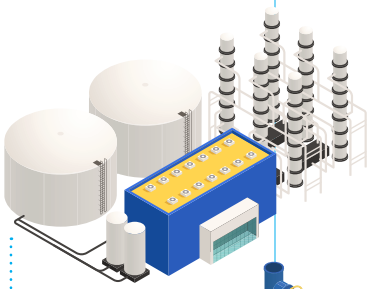
Cartografía del mundo del agua

Desde su extracción hasta su uso, pasando por su tratamiento y transporte, el curso del ciclo del agua nunca se desarrolla con normalidad. Nos sumergimos en una lista no exhaustiva de los actores de la industria del agua.

La red de agua potable

Extracción de agua sin tratar
(aguas subterráneas, masas de agua, ríos y arroyos)

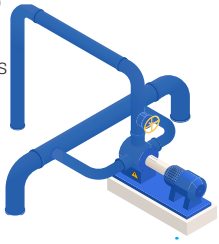




Tratamiento del agua potable
(plantas de producción de agua potable, plantas de desalinización)

Almacenamiento de agua potable
(principlamente torres de agua)

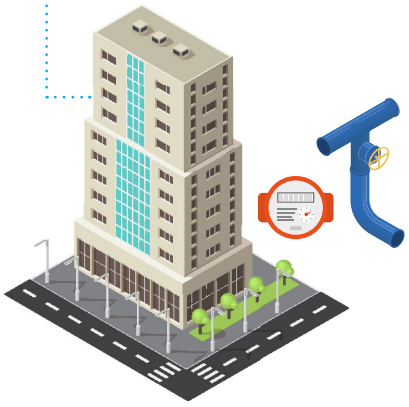




Distribución
a través de la red de tuberías

Lugares de consumo o uso

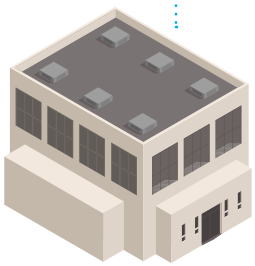
Viviendas, comercios y empresas





Granjas de cultivos y ganado

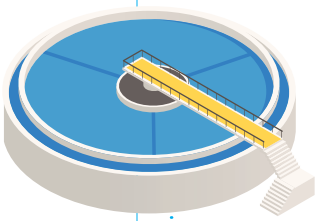
Industria



La red de purificación de aguas residuales



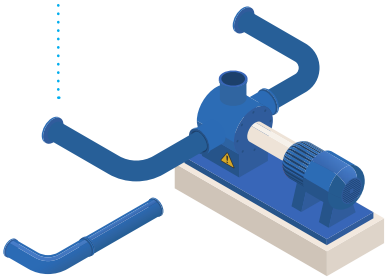
Recogida:
sistema de alcantarillado para las aguas residuales domésticas



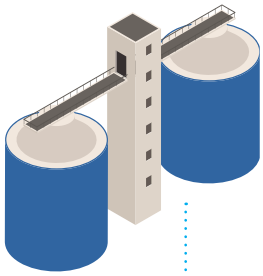
Tratamiento
plantas de reciclaje de agua

Planta de tratamiento de aguas residuales o plantas de tratamiento de aguas urbanas con tanques de tratamiento

Descarga:
sistemas de evacuación de agua purificada

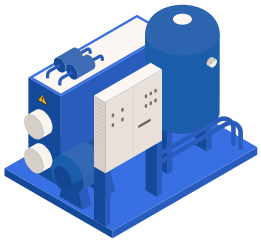


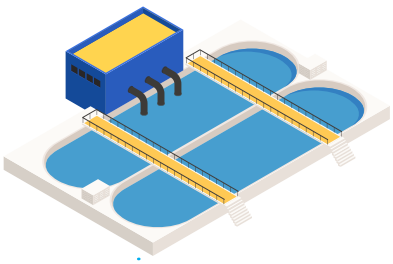
La red para agua de lluvia



Estaciones de bombeo para la defensa frente a inundaciones

Estaciones de bombeo de aguas municipales





Estanques de retención

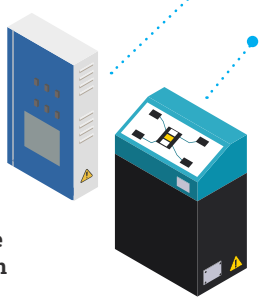
Los sistemas de información de las diferentes infraestructuras suelen ser una mezcla de muchos elementos diversos. Y todos estos elementos constituyen una importante superficie de ciberataque.

Activos fijos (estaciones de trabajo, servidores, etc.)

Estaciones de trabajo móviles



Estación de supervisión central



Dispositivos de control remoto

Sensores con comunicación IIoT (Internet de las Cosas Industrial)

Entornos en la nube



¿Por qué el sector del agua debería tomar en serio las cuestiones sobre ciberseguridad?

Parte I.

La combinación de salud pública, contaminación y geopolítica hace que las cuestiones sobre ciberseguridad en el sector del agua sean especialmente críticas. Sin embargo, a pesar de los múltiples riesgos, causados en particular por el carácter deteriorado de sus redes, el sector se esfuerza por adquirir los hábitos de seguridad digital necesarios.



Hay dos tipos principales de actores que explotan las infraestructuras del agua: las autoridades locales y las empresas privadas. Esto dificulta la elaboración de un retrato uniforme de cómo se gestionan estas cuestiones, especialmente en lo que respecta a las inversiones en ciberseguridad. Sin embargo, la cuestión es central, dado que más de 3 de cada 5 vulnerabilidades del sistema de información industrial pueden dar lugar a la indisponibilidad total de la herramienta de producción si se explotan eficazmente (fuente: informe Claroty 2020).

Los sistemas operacionales del sector del agua, envejecidos y poco actualizados, presentan más del doble de vulnerabilidades que el sector sanitario (según el mismo informe de Claroty).

Pero pocas empresas del sector del agua dan a conocer abiertamente los ciberataques que frustran o de los que son víctimas. A diferencia de otros sectores, como el del transporte o la energía, los actores del sector del agua apenas están empezando a unirse para debatir estas cuestiones de ciberseguridad. No obstante, cabe mencionar la labor de seguimiento de la red Water ISAC, activa desde 2002 en Estados Unidos, y la Association Scientifique et Technique pour l'Eau et l'Environnement (ASTEE) de Francia, que inició un grupo de trabajo sobre ciberseguridad en 2021.

Sin embargo, el sector no se ha librado, como demostró el caso de una reserva de agua de Florida en febrero de 2021. El muy publicitado (y frustrado) ciberataque en la pequeña ciudad de Oldsmar demuestra la falta de seguridad de un cierto número de infraestructuras hídricas: el ciberdelincuente pudo aprovechar un software de control remoto (TeamViewer) y cambiar el ajuste para el hidróxido de sodio, utilizado para regular el pH en la red de tratamiento del agua. Afortunadamente para los 15.000 residentes de Oldsmar, un agente de la estación detectó

> ***"En un mundo cada vez más conectado y obligado por la epidemia de Covid-19 a realizar cambios rápidos, un problema de ciberseguridad puede generar rápidamente un problema de seguridad física, o incluso plantear la cuestión de la seguridad nacional en ciertos casos extremos"***
>
> **Khobeib Ben Boubaker**
> Jefe de la Línea de Negocio de Seguridad Industrial, Stormshield

rápidamente la anomalía (11.100 partes por millón en lugar de 100), y corrigió la concentración. Es cierto que los dispositivos integrados en estos entornos para la seguridad operativa pueden actuar como salvaguardas, pero el historial de ciberataques contra el mundo del agua nos demuestra que los ciberdelincuentes son capaces de saltárselos.

Aunque, histórica y culturalmente, l**a seguridad personal siempre ha tenido prioridad sobre la seguridad informática** en el sector del agua, hoy en día ambos temas tienden a fundirse en uno solo.

La naturaleza específica de las ciberamenazas en el sector del agua surge de las motivaciones de los ciberatacantes. Este sector sensible no es muy lucrativo y, por lo tanto, rara vez es objeto de ataques con fines de lucro. Sin embargo, puede ser objetivo de maniobras mediáticas, como ocurrió en enero de 2021 en California: un ciberdelincuente consiguió borrar algunos programas utilizados por una fábrica de la bahía de San Francisco en los procesos de tratamiento del agua potable.

Pero, sobre todo, un ataque a las infraestructuras hídricas de una región sigue siendo una potente herramienta de auténtica desestabilización que puede utilizarse con fines políticos, como veremos en la siguiente sección.—

¿Un futuro de (ciber) guerras del agua?

Parte II.

Como recurso vital, el agua siempre ha ocupado un lugar estratégico en las relaciones internacionales. Esta dimensión geopolítica se ve reforzada por el cambio climático en marcha, que está transformando el "oro azul" en un recurso cada vez más preciado.



En un momento en el que los sistemas de suministro y tratamiento de agua están generalmente conectados a otras redes (en este caso, las informáticas), su vulnerabilidad es cada vez mayor. En Europa, esto explica que algunas infraestructuras de este sector tengan el estatus de "Operador de Servicios Esenciales" (OES) y deban cumplir los requisitos regulatorios. En Francia, por ejemplo, este estatus se completa con otro que designa a los "operadores de vital importancia", acompañado en este caso de estrictas obligaciones regulatorias.

Por ello, la ciberseguridad en el sector del agua es especialmente crítica, ya que contribuye a la seguridad de una actividad necesaria para la supervivencia y la salud pública. El control en este ámbito es también una muestra de la soberanía de un país.—

El ejemplo Israel y las tres olas de ataques en un año

La situación geopolítica y geográfica de Israel agrava los problemas relacionados con el agua. Esta situación ha hecho que – junto con los países del Golfo – dependa de la tecnología. Por ejemplo, el 80% del agua potable que se consume en Israel procede de plantas desalinizadoras.

En marzo de 2020, Israel frustró una serie de ciberataques que pretendían hacerse con el control de los sistemas de control industrial de varias de sus instalaciones de agua. Al parecer, el objetivo de estos ataques era aumentar los niveles de cloro en el agua (para hacerla peligrosa para el consumo) y provocar el cierre automático de las bombas. Esto habría privado a varios miles de habitantes del acceso al agua durante un periodo de intenso calor. El gobierno israelí responsabilizó a Irán y parece haber llevado a cabo un ciberataque de represalia contra el puerto iraní de Shahid Rajaee como respuesta.

Dos meses más tarde, las bombas de agua agrícolas fueron objeto de una segunda oleada de ataques, pero no sufrieron daños. Por último, en diciembre de 2020, los ciberatacantes irrumpieron en un depósito de agua aprovechando una interfaz hombre-máquina (HMI) mal protegida.

Estos ejemplos israelíes muestran hasta qué punto los ciberataques son hoy en día parte integrante de los arsenales de los Estados en conflictos más o menos abiertos o en labores de inteligencia. En otro ámbito, Rusia y China han sido señalados recientemente tras los ciberataques contra la Agencia Europea del Medicamento (EMA) en 2020.—



¿Está el sector del agua preparado para la ciberguerra?

En general, los niveles de ciberprotección en el sector del agua varían. Aunque algunos operadores llevan varios años incluyendo criterios de ciberseguridad en sus licitaciones, el riesgo cibernético sigue estando infravalorado a nivel de las autoridades locales. Esto explica en parte que ataques relativamente básicos puedan infectar a veces los sistemas industriales. Sin embargo, todo el sector del agua parece ahora decidido a ponerse al día con otros sectores, como la energía y la banca, que habían sido más rápidos en concienciarse.

"*En Francia, desde la aprobación de la Ley de Ordenación Militar y la Directiva Europea NIS, los ministerios y la ANSSI han realizado una gran labor de sensibilización de las autoridades locales y las empresas competentes en esta materia.*, explica David Giorgis, Director regional de seguridad IT y OT, Francia y director de TI industrial en Suez Francia. *Anteriormente, la ciberseguridad recibía menciones superficiales en las licitaciones redactadas por las autoridades locales, con algunas excepciones. Hoy en día, el tema ocupa a menudo varias páginas, y se espera que las respuestas incluyan documentación justificativa. Es el signo de una concienciación tranquilizadora y de unas competencias crecientes para el futuro."*—

Entrevista 1 a un cliente

Punto de vista: la ciberseguridad, un hábito que el sector del agua está aprendiendo a adquirir

David Giorgis, director de seguridad TI y OT y director de TI industrial en Suez Francia, tiene un asiento de primera fila desde el que observar los avances en la industria del agua. Pudimos hacerle algunas preguntas y bucear con él por debajo de la superficie de la industria de la ciberseguridad.

David Giorgis — *"Alrededor del 90% de los ciberincidentes que observamos están relacionados con la informática de gestión; es decir, ofimática, puestos de trabajo, mensajería, aplicaciones. Hay que decir que nuestro CRM contiene los datos de millones de clientes directos, y que nuestro SI debe ser accesible para el seguimiento del consumo, entre otras cosas. Todos estos son activos que requieren ser protegidos además de las vulnerabilidades tradicionales relacionadas con la mensajería, por ejemplo*

Afortunadamente, en los proyectos informáticos de Suez, el enfoque de seguridad por diseño es ya universal. En los proyectos puramente industriales, este hábito aún no se ha adoptado en todas partes, porque a menudo se gestionan localmente y la ciberseguridad se está desarrollando para convertirse en parte integrante de la cultura. Esto significa que estos proyectos de OT son cada vez más seguros, por lo que Suez está aplicando un enfoque integral de la ciberseguridad para obtener el máximo rendimiento operativo.

La dificultad que encontramos, al trabajar en la ciberseguridad de los sistemas operativos está muy a menudo relacionada con los protocolos industriales. En efecto, algunos grandes fabricantes han aportado características específicas a los protocolos estándar, y las herramientas de seguridad están mejorando para tenerlas en cuenta. El análisis es por tanto limitado, hasta

que el desarrollador de soluciones de ciberseguridad desarrolle un módulo específico. Por tanto, es importante que los actores del sector trabajen juntos.

Como parte de sus funciones, David Giorgis trabaja regularmente con las comunidades de clientes de Suez Francia. Le hemos preguntado cuáles son las recomendaciones más habituales publicadas en el ámbito de la ciberseguridad industrial del agua:

DG — *"Una nueva colaboración siempre comienza con un análisis del sistema existente, para garantizar que la información disponible se ajusta a la realidad. Después, solemos iniciar una fase de negociación para renovar los equipos obsoletos y actualizar los existentes. En realidad, el objetivo es estar "lo más actualizado posible": a veces nos vemos obligados a conservar sistemas operativos antiguos, porque las aplicaciones empresariales no son compatibles con las versiones más recientes de estos SO.*

La otra gran área de mejora es la segmentación de la red operativa. Esto representa mucho trabajo. También es importante separar los SI industriales y los SI de gestión (una regla clave para Suez) o, si hay que hacer una excepción, garantizar la seguridad de las interfaces entre ambos. Esto requiere el despliegue de unos fundamentos de seguridad básicos (antivirus, actualización, cortafuegos, etc.). Se trata de acciones totalmente estándar en el mundo de la informática de gestión, pero todavía novedosas en el sector industrial en general, y del agua en particular."

La envergadura de la tarea lleva a preguntarse cómo se sienten los equipos sobre el terreno: ¿perciben en general la ciberseguridad como un impedimento para sus proyectos?

DG — *"En los últimos años se ha hablado mucho más de los problemas de ciberseguridad, por lo que, en general, los equipos industriales son muy conscientes de su importancia. Yo añadiría que el papel del responsable de la seguridad de los sistemas de información no es impedir un proyecto, sino apoyarlo para que tenga en cuenta las condiciones de seguridad relevantes. Nuestra filosofía consiste en orientar a los especialistas en informática industrial sobre el terreno hacia soluciones integradas, seguras y de ámbito nacional. Nuestros equipos centrales y nuestra filial Suez Smart Solutions, especializada en los sistemas industriales y su ciberseguridad, también están disponibles para ayudarles en la implantación de estas soluciones."*—

Un enfoque pragmático y de colaboración que, en última instancia, busca establecer la ciberseguridad como una función de apoyo eficaz en la vida diaria de los equipos operativos.

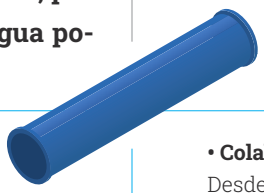
¿Cuáles son los cuestiones que impulsan la ciberseguridad en el sector del agua?

Parte III.

Además de los motivos a nivel de estado o de delincuencia, ¿qué hace que la industria del agua sea un objetivo principal para los ciberatacantes? Hemos enumerado los principales cuestiones sobre ciberseguridad en el sector desde tres perspectivas: humana, tecnológica y operativa.



Para empezar, hay que señalar que en el sector del agua, el principal objetivo de la ciberseguridad es garantizar la disponibilidad y la integridad de los procesos industriales. El concepto de confidencialidad también entra en juego, pero en el contexto menos crítico de la relación con el cliente: la integridad de los datos es muy importante en términos de telemetría para garantizar una facturación precisa, pero las cuestiones son de un orden de magnitud diferente cuando se trata, por ejemplo, de garantizar el suministro de agua potable.



Perspectiva humana

• Los riesgos humanos de importancia son inherentes al sector

Como hemos detallado en el apartado anterior, el suministro de agua potable y el tratamiento de las aguas residuales son actividades críticas, ya que son necesarias para la supervivencia y la salud humanas. Las consecuencias de la rotura de una presa o de la contaminación del agua serían realmente dramáticas.

• Los riesgos de los errores o actos maliciosos

Por estas razones, el componente humano – ya sea fruto de un error o de un acto malintencionado – es uno de los componentes más temidos por las empresas y los operadores industriales, y exige la elaboración de diferentes escenarios para una seguridad operativa óptima.

• Colaboraciones ocasionalmente complejas

Desde el punto de vista empresarial, la gestión coordinada de la ciberseguridad informática y operativa presupone la capacidad de satisfacer las necesidades del ingeniero de automatización al tiempo que se reducen los riesgos identificados por el CISO o el responsable de seguridad informática.

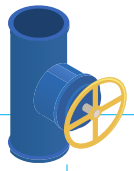
Desde el punto de vista organizativo, por ejemplo, es frecuente que varios agentes trabajen en régimen de delegación para una misma zona urbana. La propia zona urbana puede conservar parte de la gestión interna. El resultado en estos casos es un verdadero ecosistema de gestión del agua cuyos actores deben aprender a trabajar juntos.

• Ámbitos que suelen excluir la ciberseguridad industrial

Al igual que en otros sectores, es habitual que los equipos encargados de la ciberseguridad operativa se sitúen bajo la responsabilidad del director de la planta, en lugar de estar en el ámbito del responsable local de TI. En otros casos, el responsable de TI recomendará a veces normas cibernéticas que el operador del servicio es libre de aplicar. O no.....-

> ***"Las redes industriales a veces no se tienen en cuenta a la hora de evaluar los riesgos de ciberseguridad o de recuperarse de un ciberataque"***

Tarik Zeroual
Global Account Manager, Stormshield



Perspectiva tecnológica

• Una línea difusa entre la ciberseguridad informática y la industrial

Con el fin de la RTPC (red telefónica conmutada), la industria del agua está migrando gradualmente a tecnologías de comunicación como Ethernet, 4G e incluso 5G. Esta evolución forma parte de una tendencia global de convergencia entre las TI y las OT en los últimos años. Por lo tanto, esto deja a las redes industriales más expuestas que antes, ya que han entrado en el perímetro de un potencial ciberataque a través de la red informática.

• Una Internet de las cosas Industrial (IIoT) a proteger

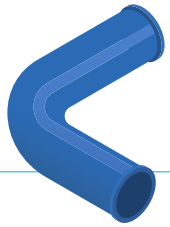
La IIoT se refiere a cualquier objeto conectado que envía información (temperatura, válvula abierta, nivel de cloro, etc.) a una máquina. Estos sensores "inteligentes" relativamente baratos son muy fáciles de integrar en los sistemas existentes, lo que explica su éxito en los entornos industriales. Desgraciadamente, también son muy vulnerables, ya que todavía es demasiado raro que se tengan en cuenta las cuestiones de ciberseguridad en el momento de su diseño.

• La protección debe extenderse a los entornos virtuales

Con la adopción de la nube – sobre todo cuando se abastece de datos mediante la IIoT – y el uso de máquinas virtuales, se ha externalizado toda una parte de los sistemas de información de las empresas de agua. Por lo tanto, es vital proteger estos enlaces en la nube para evitar ataques de ciberespionaje contra la infraestructura de los centros industriales. Sin embargo, esto requiere identificar claramente si la responsabilidad de esta tarea recaerá en las unidades de negocio o en los servicios gestionados.–

> ***"El mantenimiento predictivo es una de las principales aplicaciones operativas de la IIoT. Los datos retroalimentados por los sensores se utilizan para los cálculos de predicción, eliminando el mantenimiento innecesario y reduciendo la probabilidad de fallos"***

Tarik Zeroual
Global Account Manager, Stormshield



Perspectiva operativa

• Fuertes diferencias de madurez
En Europa, la consideración de los problemas de ciberseguridad en las infraestructuras hídricas varía mucho en función del nivel de concienciación y de los recursos de la autoridad responsable.

• La multiplicidad de ubicaciones: una fuente clave de cibercomplejidad en el sector
En la práctica, ofrecer ciberseguridad a las infraestructuras hídricas críticas no es fácil, ya que se trata de un sector muy descentralizado que se ve obligado a operar en múltiples emplazamientos para abastecer a toda la zona geográfica. Las conexiones a Internet y el mantenimiento a distancia plantean, por tanto, importantes problemas relacionados con los métodos de acceso remoto que garantizan el correcto funcionamiento de los emplazamientos remotos.

• Una ciberimplantación difícil sobre el terreno
Debido a su distribución fragmentada, algunas infraestructuras del sector del agua tienen limitaciones específicas, como la humedad o la temperatura.

• Equipos de producción sensibles
No es raro encontrar que un dispositivo automático en funcionamiento en una planta de tratamiento de aguas residuales tenga ya 10, 15 o incluso 20 años. Estos dispositivos envejecidos rara vez cuentan con mecanismos de ciberprotección integrados y utilizan protocolos industriales inseguros, por lo que son vulnerables.

• Uan arquitectura de red permeable
Estos sistemas se organizan todavía con demasiada frecuencia según una arquitectura de red "plana", es decir, sin partición ni segmentación. Esto supone un riesgo real en cuanto a la propagación de malware.

• Una importante limitación de tiempo
La sensibilidad de estos equipos se debe también a la limitación que supone el funcionamiento en tiempo real. En la industria del agua, es esencial que cada operación se desencadene de forma instantánea y, por tanto, que se minimice el tiempo entre la instrucción y la acción. Los equipos de seguridad deben, por tanto, generar la menor latencia posible, para evitar la interrupción del proceso industrial – lo que podría suponer una parada de la producción.

• Una variedad de partes interesadas, que puede difuminar la visibilidad
Dada la antigüedad de la mayoría de los sistemas industriales de agua, el operador actual no siempre tiene acceso al historial de modificaciones. El uso de numerosos proveedores de servicios, operadores e integradores también sirve para acentuar este fenómeno.—

> ***"Estas redes distribuidas también son más propensas a la intrusión física. Esto significa pensar de manera diferente sobre la ciberseguridad. Esta cuestión de seguridad física añade complejidad al enfoque de la ciberseguridad de una planta de tratamiento de aguas residuales o de una torre de agua"***

Vincent Nicaise
Responsable de partner y ecosistema industrial Stormshield

Infografía

Las principales vulnerabilidades en el sector

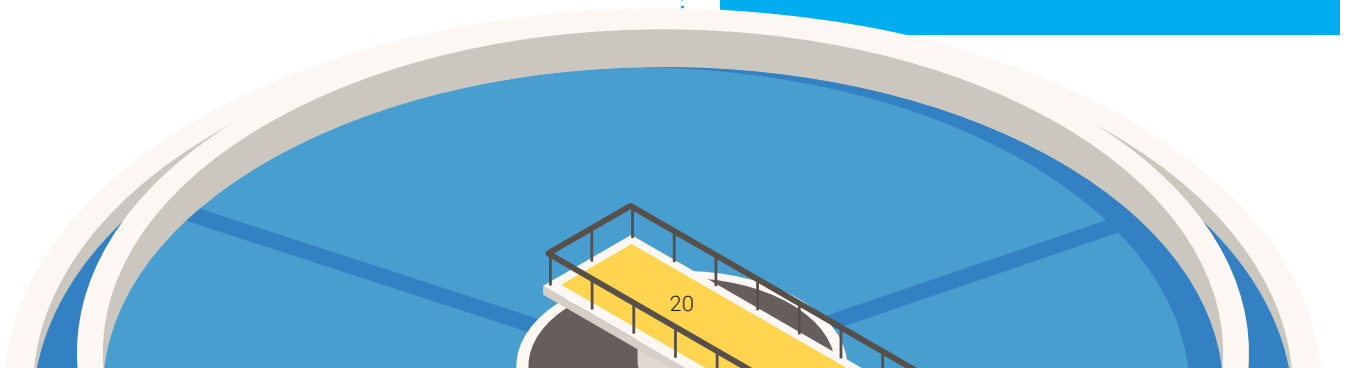
En los últimos años, las preocupaciones de los profesionales de la ciberseguridad se han centrado especialmente en el despliegue del "Internet industrial de las cosas" (IIoT). Sin embargo, esto no debe significar pasar por alto un cierto número de vulnerabilidades estructurales en estos sistemas industriales.

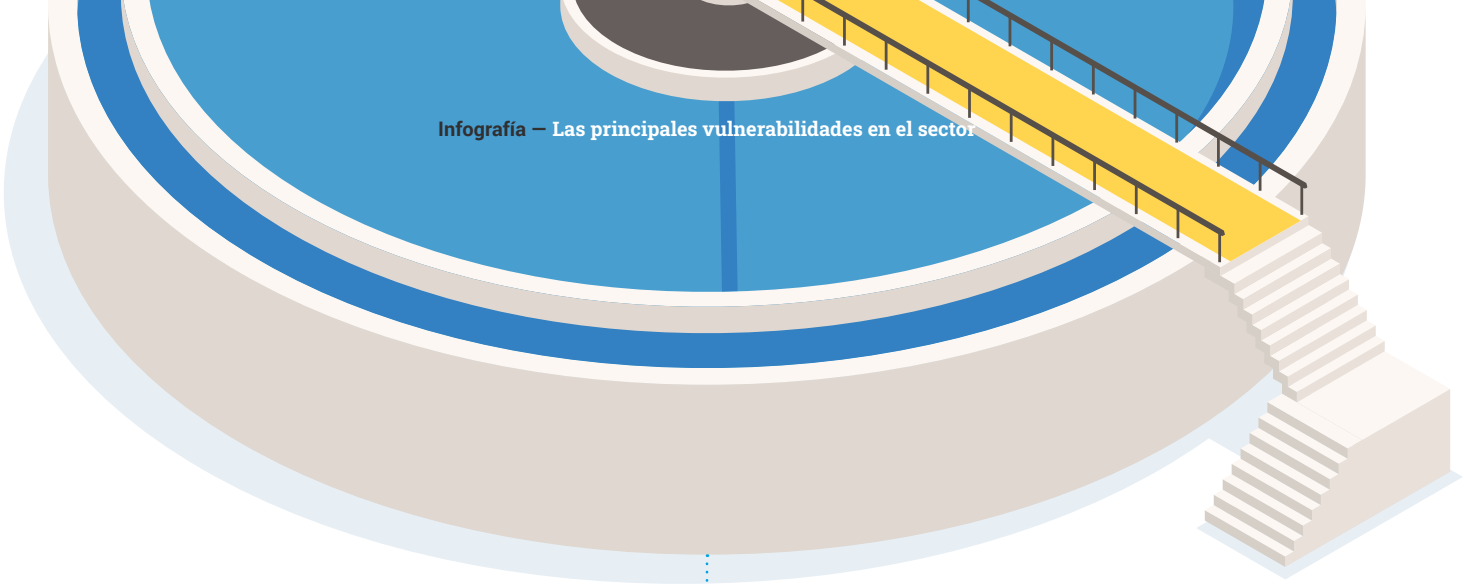
Los sistemas de control industrial (ICS) en general pueden presentar vulnerabilidades a varios niveles:

Los equipos en operación (software, hardware y firmware)

tienen tecnologías dispares, anticuadas y/o inseguras. Entre ellas se encuentran las siguientes: el DCS (*Sistema de Control Distribuido*), las interfaces hombre-máquina (HMI), los controladores lógicos programables industriales (PLC), las soluciones de control y adquisición de datos SCADA y otro software de supervisión, así como los sensores IIoT y las plataformas en la nube con las que se comunican. En conjunto, forman una superficie de ataque considerable.

En febrero de 2020, se descubrió una vulnerabilidad en los HMI C-more del fabricante estadounidense AutomationDirect. Estos HMI son utilizados, entre otros, por operadores del sector del agua. Aprovechando este fallo (CVE-2020-6969), los ciberdelincuentes pudieron descubrir credenciales y otra información sensible en archivos de proyectos desprotegidos.—





Infografía — Las principales vulnerabilidades en el sector

En la red y en sus periféricos

Diseñadas a menudo según una arquitectura "plana", las redes industriales no siempre están aisladas unas de otras, según los principios de segmentación. Además de ser un terreno fértil para la propagación de malware, los equipos de red tienen nuevas vulnerabilidades cada día – porque están obsoletos y se actualizan con poca frecuencia. Estas vulnerabilidades también pueden ser introducidas por la gestión remota, que todavía se realiza con demasiada frecuencia de forma insegura.

En los sistemas operativos para monitorizar o programar estaciones

Estos sistemas fuera de línea quedan obsoletos desde el punto de vista cibernético debido a la falta de actualizaciones. Pero estos sistemas son también los únicos que ejecutan algunas aplicaciones de negocio históricas, que son incompatibles con los sistemas más recientes.

En los protocolos

El uso de protocolos no cifrados e inseguros, como Modbus, es habitual en la supervisión industrial.

En los usuarios

Los operadores y mantenedores a cargo del proceso industrial aún no tienen todos una gran conciencia de las cuestiones de ciberseguridad. Esto significa que las políticas de gestión de usuarios, contraseñas y accesos son aspectos que se utilizan demasiado poco en los sistemas industriales.–

¿Qué ciber regulaciones existen en el sector del agua?

Parte IV.

Además de su estricta supervisión sanitaria y medioambiental, el sector del agua está sujeto la ciber normativas nacionales e internacionales.



> ***Con la aplicación de los decretos en 2016, empezamos a ver una aceleración de la ciber-conciencia por parte de los operadores franceses. Con las autoridades locales, se tardó un poco más y vimos los primeros cambios en este ámbito entre 2017 y 2018***
>
> **Khobeib Ben Boubaker**
> Jefe de la línea de negocio de seguridad industrial, Stormshield

Además de su estricta supervisión sanitaria y medioambiental, el sector del agua está sujeto la ciber normativas nacionales e internacionales.

Teniendo en cuenta los retos de salud pública descritos anteriormente, es fácil ver cómo la actividad de ciertos actores del sector se considera crítica. En Francia, los actores encargados del suministro y la distribución de agua potable tienen el estatus de OIV (operadores de importancia vital) en el sentido de la Ley de Planificación Militar (LPM) (2013). Por lo tanto, deben cumplir las 20 normas establecidas por la LPM para los SI más críticos: cartografía de los SI, supervisión, normas de identificación y autenticación, notificación de incidentes, uso de soluciones de seguridad cualificadas al más alto nivel, etc.

A nivel europeo, también pueden identificarse como OSE (operadores de servicios esenciales) en virtud de la Directiva NIS (2016). Francia había tomado un poco de ventaja durante su transposición a la legislación nacional para incluir a los actores del saneamiento: La armonización europea está en camino, ya que se espera que este sector se incluya en el texto de la directiva durante su revisión prevista a finales de 2021, al igual que con la gestión de residuos.

Por último, algunas organizaciones – a menudo pequeñas autoridades locales – no se consideran ni OIV ni OSE: sin obligaciones normativas, actúan por tanto en función de sus recursos y de su nivel de conciencia de la amenaza. Para ayudarles, la ANSSI ha publicado varias guías de buenas prácticas para la autoevaluación y la auto-seguridad. Y para los que quieran ir más allá, existen muchas normas, como la norma internacional de ciberseguridad industrial IEC 62443-3-3 y el marco del NIST estadounidense.—

¿Y qué pasará mañana?

Parte V.

Lo digital es un motor importante en la protección del agua: tomar sólo lo necesario, minimizar la huella medioambiental de las fábricas y garantizar el suministro de agua de calidad sin fugas son retos que aumentarán en los próximos años.



En sus esfuerzos por mejorar el funcionamiento de las perforaciones y las bombas con el aprendizaje automático, captar las señales débiles que advierten de la sequía y predecir los caudales futuros, el sector del agua recurre cada vez más a la tecnología.

Con la continua digitalización del sector, los límites entre TI y OT seguirán difuminándose, lo que aumentará el riesgo cibernético al que el sector ya está expuesto. Por ello, el sector del agua debe elevar sus niveles de ciberseguridad y organizar su ciber-resiliencia para poder hacer frente a ataques cada vez más frecuentes y peligrosos.

Un público totalmente educado y una normativa más estricta

Por lo tanto, en el futuro, la ciberseguridad debe ser una parte integral del mantenimiento del proceso industrial. Esto representa una tarea importante; hay que proteger casi toda la infraestructura actual. Pero hay signos alentadores. En apoyo de este proceso, la tendencia de los próximos años será reforzar el marco normativo de la ciberseguridad – según David Giorgis, director de seguridad de TI y OT y director de TI industrial de Suez Francia. En su opinión, la próxima revisión de la directiva NIS es un primer paso al que seguirán, entre otros, numerosos ajustes en la Ley de Planificación Militar de Francia. La cooperación transfronteriza debería ser uno de los ejes principales de esta nueva normativa, cuya ambición – según la agencia de ciberseguridad ANSSI – es "*mejorar la ciber-resiliencia de la Unión Europea y sus miembros*".

> ***"Los integradores de automatización están abordando cada vez más los retos de los sistemas industriales. También es alentador ver el número de licitaciones para el diseño o la renovación de sistemas que ahora incluyen un componente cibernético"***
>
> **Vincent Nicaise**
> Repsonsable de partner y ecosistema industrial, Stormshield

Así que vale la pena obtener una ventaja temprana siguiendo los consejos de Tarik Zeroual, Global Account Manager de Stormshield, que ahora recomienda "*ir más allá del cumplimiento normativo mínimo*".

Soluciones tecnológicas de probada eficacia

El futuro del sector del agua estará inevitablemente teñido de ciberamenazas, pero los desarrolladores y los investigadores de ciberseguridad trabajan duro para ofrecer soluciones que aborden tanto los problemas recurrentes como los emergentes.

• Proteger las redes a través de la segmentación
La segmentación de la red es esencial porque ayuda a evitar la propagación de un ciberataque al aislar los subsistemas. Para ello se pueden utilizar cortafuegos como los de la gama Stormshield Network Security (SNS).

• Autorización del tráfico
También es importante disponer de soluciones capaces de verificar la legitimidad de los comandos emitidos por los PLC. "*No solo para protegerse de los ataques de intermediario, sino también para verificar la integridad de los datos mediante inspección*", afirma Stéphane Prévost, director de marketing de producto de Stormshield.

• Gestionar el acceso remoto

En un sector con infraestructuras que a veces pueden estar muy alejadas unas de otras, es imperativo establecer sistemas para gestionar y asegurar el acceso remoto (mantenimiento remoto, gestión de alarmas, etc.). Para garantizar la seguridad de las comunicaciones entre los distintos emplazamientos y máquinas, la solución SNS se encarga del cifrado de los datos mediante la creación de túneles VPN y la autenticación de los usuarios.

• Obtener una visión general

Para facilitar la gestión de múltiples soluciones SNS distribuidas, Stormshield ha desarrollado una plataforma de gestión centralizada denominada Stormshield Management Center (SMC). Stormshield también ofrece una solución de gestión de registros de log – Stormshield Log Supervisor (SLS) – que ofrece una mejor visibilidad sobre el estado y los registros de log de las redes informáticas. Estas soluciones también tienen en cuenta el aumento del tráfico entre las TI y las OT, gracias a una política de seguridad unificada entre los dos entornos.

• Proteger los puntos finales

La protección de los puntos finales es esencial, ya sean estaciones de trabajo de ingeniería o de supervisión, debido a su papel clave en el manejo de los parámetros del proceso operativo y en la visión en tiempo real del estado de los sistemas. Por ejemplo, un ciberataque a las estaciones de supervisión dejaría a los equipos operativos completamente "a ciegas" e impediría el correcto funcionamiento de los procesos industriales. Por ello, la solución Stormshield Endpoint Security (SES) combina un motor de análisis de comportamiento, un motor de control de dispositivos y la capacidad de realizar listas blancas de aplicaciones, deshabilitando cualquier software que no sea estrictamente necesario para ofrecer una mejor protección.

• Adaptación de los equipos a las limitaciones del sector del agua

El sector del agua tiene una serie de limitaciones físicas específicas (alta humedad, amplios rangos de temperatura, aislamiento de ciertos lugares, etc.), además de las limitaciones operativas para la continuidad de la actividad. Por lo tanto, esta industria requiere equipos capaces de responder a estas limitaciones ambientales. La funcionalidad de los cortafuegos SNS y su funcionalidad de bypass (modo de seguridad) son también potentes activos para la industria del agua, ya que garantizan la disponibilidad del proceso operativo.

• Esforzarse por lograr la *seguridad desde el diseño*, incluso para las OT. El enfoque de *seguridad desde el diseño* consiste en abordar las

Soluciones de cortafuegos industriales SNi40 y SNi20:

Stormshield ha colaborado con Schneider Electric en el diseño de carcasas reforzadas que responden a los requisitos de entornos muy exigentes, como el sector del agua. Optimizados para bajas latencias inducidas y equipados con una funcionalidad de bypass (un modo de seguridad que permite el mantenimiento en servicio), pueden instalarse fácilmente en la proximidad física de los equipos a proteger, y pueden soportar los entornos específicos de este sector. A nivel normativo, los cortafuegos SNi20 y SNi40 cuentan con la calificación Standard de la ANSSI – prueba de su robustez y fiabilidad.—

cuestiones de ciberseguridad desde la primera fase de diseño del sistema. Se trata de un enfoque más relevante – y preferible – en el sector del agua, dada la integración a posteriori de las medidas de ciberseguridad. Esto se debe a los tiempos de desarrollo relativamente largos, a los problemas de las bases de usuarios instaladas, que son incluso mayores que en la ofimática, y a los numerosos retos técnicos de compatibilidad con los activos existentes. Por ello, los integradores y expertos son muy conscientes de que la seguridad desde el diseño es la clave para una industria mejor protegida en el futuro.

Nuevos perfiles para ofrecer ciberseguridad en el sector del agua

Como hemos visto, ofrecer ciberseguridad en el sector del agua significa hoy en día depender de más y más herramientas. Por lo tanto, se necesitan muchas habilidades diferentes para captar, entender y hacer el mejor uso de estos recursos.

Para que los equipos de vigilancia e intervención (CSIRT, SOC, etc.) tengan acceso a las mejores competencias, es importante que los especialistas en automatización se formen en ciberseguridad informática. Y a la inversa, para que los especialistas en ciberseguridad se familiaricen con la parte industrial.—

> ***"Precisamente porque queremos que nuestros equipos se conozcan y trabajen mejor juntos, cada año realizamos un ejercicio cibernético, con un escenario que incluye sistemas industriales, y con la participación de nuestros especialistas en OT"***
>
> **David Giorgis**
> Director regional de seguridad IT y OT, Francia y director de TI industrial en Suez Francia



Puede que los sistemas de TI y OT estén convergiendo, pero ¿está en marcha el mismo proceso entre sus respectivos equipos humanos? El tiempo lo dirá, pero la ciberseguridad en el sector del agua en los próximos años parece depender de la capacidad de los expertos en industria y ciberseguridad para trabajar juntos en la co-construcción de soluciones relevantes.

¿Tiene un problema complejo de ciberseguridad? ¿Un proyecto de seguridad que implica una infraestructura específica? Nuestros expertos internos están aquí para discutirlo y proporcionarle el soporte que necesita.

Póngase en contacto con nosotros.

Entrevista a un cliente

Proteger una red distribuida: cómo mejorar la ciberseguridad de la autoridad del agua de una ciudad

Las autoridades municipales de una importante región francesa ha optado por confiar la gestión del servicio público de producción, transporte, almacenamiento y distribución de agua potable en la mayor parte de su zona geográfica de responsabilidad a un único interlocutor, tras varios años de trabajo con tres operadores diferentes.

1,3
millones de habitantes

60
municipios

100
torres de agua

Modernizar su infraestructura informática y aumentar su nivel de seguridad

Este proceso de racionalización de los servicios también ha brindado a la autoridad municipal la oportunidad de revisar su arquitectura informática, haciéndola más moderna y segura.

El operador principal seleccionado por el cliente acudió a Stormshield para que le apoyara en la seguridad de este entorno industrial y en la implementación de las funcionalidades clave requeridas; es decir, el control y el filtrado de cada comunicación (utilizando *Inspección profunda de paquetes*, DPI – y con especial atención al protocolo Modbus) y la implementación de una solución VPN IPSec para proteger las comunicaciones.

Se configuraron los cortafuegos para segmentar y proteger mejor las distintas redes operativas (red de oficinas de TI, concentradores centrales de VPN, TI industrial y de seguridad, y también sitios remotos).

Una respuesta industrial adaptada a las limitaciones del sector del agua

Por ejemplo, la seguridad en la sede central se ha reforzado con la instalación de cortafuegos entre la red de oficinas y las instalaciones de negocio. Estas instalaciones están repartidas en dos redes distintas (seguridad e industrial), cada una de ellas protegida por un conjunto de cortafuegos diseñados para actuar como concentradores de VPN.

Esta arquitectura interconecta estas mismas aplicaciones a las diferentes torres de agua, que fueron equipadas individualmente con dos grupos de cortafuegos reforzados SNi40, asegurando los flujos entre los diferentes sitios y aplicaciones.

El cliente también quedó muy impresionado con la funcionalidad DPI con estados de los protocolos industriales, que llevará la seguridad de estos sistemas sensibles a un nuevo nivel, en paralelo con las infraestructuras modernizadas.

Servicios diseñados para estos complejos entornos industriales

Para garantizar el servicio a los usuarios y abordar las cuestiones de accesibilidad y sensibilidad en determinados luegares, Stormshield y el operador seleccionado han establecido mecanismos de soporte adecuados, entre ellos

- La implementación de un procedimiento que permite a un agente técnico sin conocimientos de redes/seguridad sustituir un cortafuegos que falla y restablecer el estado operativo del sitio con el nivel de seguridad adecuado,

- la activación de la funcionalidad de bypass (un modo de seguridad que permite el mantenimiento en servicio) en el 5% de los sitios que están equipados con un único cortafuegos en lugar de un clúster,

- una serie de servicios profesionales para apoyar a la autoridad municipal en su proceso de industrialización de las configuraciones en los sitios piloto iniciales.—

Los tres factores clave para una respuesta eficaz

- Una fuerte implicación de la **asociación operador/desarrollador**, lo que permite gestionar el proyecto y garantizar el despliegue con éxito y rapidez de principio a fin.

- Una **oferta industrial de Stormshield que se adapta** tan bien a la gestión de sitios estándar como a entornos con fuertes restricciones industriales (temperatura, humedad, carriles DIN, alimentación industrial, bypass).

– Un **único firmware unificado** desplegado en toda la gama Stormshield Network Security y una **única consola de gestión**, Stormshield Management Center, para gestionar todos los activos de cortafuegos.—

STORMSHIELD

La elección Europea para ciberseguridad



En todo el mundo, las empresas, las instituciones gubernamentales y las organizaciones de defensa necesitan poder contar con socios de confianza para apoyar su transformación digital y proporcionar ciberseguridad a sus infraestructuras, usuarios y datos. Las tecnologías de Stormshield están certificadas al más alto nivel europeo (EU Restricted, NATO Restricted, Common Criteria EAL3+ / EAL4+, calificaciones y visados de ANSSI), y abordan los desafíos de TI y OT para proteger su actividad empresarial. N**uestras soluciones de seguridad le devuelven la libertad de hacer negocios con total tranquilidad.**

www.stormshield.com

Queda prohibida toda distribución, reproducción o representación, incluso parcial, de este libro blanco, para cualquier fin que no sea el uso privado, independientemente del soporte, y puede comprometer la responsabilidad civil y penal de cualquier persona que incumpla esta prohibición.