La ciberseguridad en la gestión inteligente del agua

Lacroix Sofrel analiza las medidas destinadas a proteger las instalaciones, los equipos y las comunicaciones y *softwares* de posibles ataques cibernéticos en los proyectos hidráulicos

Sonia Contreras, responsable de Preventa y Marketing de Lacroix Sofrel España

La digitalización del mundo en el que vivimos es un hecho innegable. El sector del agua no se queda atrás: se sumerge, se zambulle y navega en la utilización de nuevas tecnologías que permiten conectar a las personas con los sistemas, haciendo más fácil el acceso a la información. Pero esta hiperconectividad no está exenta de amenazas, ciberataques malintencionados que pueden provocar crisis importantes en el funcionamiento de las instalaciones y consecuencias ambientales, repercutiendo en la calidad de servicio ofrecida al usuario y en el impacto reputacional de las empresas u organismos afectados. Con la idea de compartir y aportar un poco de luz en este asunto, Lacroix Sofrel España organizó la jornada 'La ciberseguridad en la gestión inteligente del agua' que, antes de la pandemia provocada por el coronavirus, se convirtió en un foro de encuentro donde compartir los testimonios y las experiencias de los principales expertos de ciberseguridad en este país. Este reportaje resume los principales contenidos de la jornada de Lacroix Sofrel España.

El auge de las comunicaciones del Internet of Things (IoT) en el sector del agua, con infraestructuras consideradas críticas y esenciales, y el deber de cumplir la normativa vigente (Directiva europea NIS y su transposición a la ley española), provoca que poco a poco se empiecen a desarrollar medidas destinadas a proteger las instalaciones, equipos, comunicaciones y *softwares* de posibles ataques cibernéticos, comenzando tímidamente a valorar a la ciberseguridad como un aspecto más dentro de los proyectos hidráulicos.

Según el estudio realizado por el CCI en el año 2019 con el título de 'Incidentes de ciberseguridad industrial en servicios esenciales de España', se demuestra que todavía las organizaciones que operan servicios esenciales no están suficientemente preparadas para dar respuesta a los incidentes de ciberseguridad, pero están haciendo grandes esfuerzos por mejorar sus capacidades.

Por eso, como se suele decir, aún queda mucho trabajo por hacer: es necesario contar con más políticas de concienciación, más inversiones para ayudar a las operadoras a implementar la ciberseguridad en sus proyectos, más profesionales expertos en la materia... De esta forma se conseguirán implementar estos aspectos de seguridad dentro de las redes de agua.

Con la idea de compartir y aportar un poco de luz en este asunto, Lacroix Sofrel España organizó la jornada 'La ciberseguridad en la gestión inteligente del agua'. El fin no era otro que crear un foro de encuentro para compartir los testimonios de los principales expertos de ciberseguridad en este país. Casi un centenar de profesionales asistieron al Instituto de la Ingeniería de España, en Madrid, para conocer y participar de los temas expuestos, desde explotadores de agua hasta integradores, ingenierías, consultorías y universidades.

Javier Pino, director comercial de Agua de Lacroix Sofrel en España, fue el conductor de la jornada, la cual fue inaugurada por Patrick Fabre, director de Lacroix España, y Ronald Vracken, presidente ejecutivo de Lacroix Environment y *management director* de Lacroix Sofrel. Entre ambos expusieron la actuación de esta empresa en la gestión inteligente de redes de agua como fabricante de soluciones y equipamientos tecnológicos, así como el papel protagonista que ocupa la ciberseguridad en el marco de la automatización industrial, recalcando que Lacroix Sofrel, desde hace 7 años, dispone de soluciones adaptadas para responder a estos retos.

LA CIBERSEGURIDAD EN LA INDUSTRIA ESPAÑOLA Y EL SECTOR DEL AGUA

En el primer bloque intervino José Valiente, director del Centro de Ciberseguridad industrial (CCI), que presentó cifras respecto a las vulnerabilidades entre todos los sectores, destacando que los sectores de energía y agua parecían ser los más expuestos. El motivo principal es que en estos sectores se utilizan equipamientos con tecnologías industriales "comerciales", más implantados y en consecuencia más estudiados. Entre los equipos y *softwares* más atacados se encuentran los de comunicaciones, seguidos de los sistemas de supervisión. Las consecuencias que sufren los sistemas esenciales son, sobre todo, la falta de servicio, seguido de las consecuencias medioambientales y, con un porcentaje notable y de gran importancia, el impacto reputacional.

También hizo referencia al 'Estudio de ciberseguridad en la industria española. Sectorial y regional', el cual señala las barreras iniciales de las empresas hacia la ciberseguridad:

- Desconocimiento de las propias instalaciones. Según el estudio, un 24% de las empresas no han realizado un análisis de riesgos de sus instalaciones. En el ámbito del agua, el porcentaje baja al 19%. Hay que tener especialmente cuidado en proteger los accesos a las instalaciones de manera adecuada; asegurar la cadena de suministro (por ejemplo empresas que realizan el telemantenimiento); las seguridades informáticas (*backups*, *firewalls*, antivirus…); y los procedimientos en gestión de incidentes.

- Falta de formación y cualificación del personal en el ámbito industrial. Si no hay formación, no se percibe el riesgo. En este estudio solo un 24% de las Direcciones se declara bastante concienciado con la ciberseguridad.
- Inexistencia de un responsable de ciberseguridad industrial, indispensable para coordinar cualquier proyecto relacionado.

Con su ponencia 'Comparativa: situación de ciberseguridad del sector agua *versus* otros sectores', Valiente dejó claro que la ciberseguridad es un tema esencial en todos los sectores, incluido el del agua, en el que aún queda mucho hacer.

El segundo experto fue Santiago González, analista de Ciberseguridad en el Centro Nacional de Protección e Infraestructuras y Ciberseguridad (CNPIC). Este organismo tiene como objetivo impulsar y organizar todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas y la ciberseguridad en España. Explicó que existen 12 sectores estratégicos definidos como críticos en la ley PIC, siendo el sector del agua uno de ellos y de los primeros en crear un Plan Estratégico del Sector (PES) en términos de ciberseguridad, por allá en 2015. En 2020 se está comenzando la renovación de este segundo PES.

González explicó que en España (datos 2016-2019) hay una tendencia cada más elevada de ciberataques e incidencias (*malware*, recolección de los datos, acceso de intrusión, etc.), pero cada año se dotan de más medios para detectarlos. En los últimos tiempos uno de los ataques más destacados es la disponibilidad de los sistemas relacionadas con el IoT. Para corregir estos incidentes, es necesario que los operadores trabajen la ciberresilencia, es decir, un método en el que exista un autoaprendizaje y autocorrección en los principios básicos: anticipar, resistir, recuperar y evolucionar. A disposición de los operadores críticos, existe en la web del CNPIC una guía de notificación de incidentes en la que se pautan las obligaciones y los procedimientos para notificar incidencias y medidas para solucionarlas.

Con su presentación 'Situación actual en la protección de infraestructuras críticas', González evidenció el gran trabajo que los organismos y empresas competentes realizan para que existan las medidas adecuadas para proteger las infraestructuras críticas, entre ellas las de agua.

El último ponente de este bloque fue Enrique Redondo Martínez, responsable de Ciberseguridad Industrial del Instituto Nacional de Ciberseguridad (INCIBE), organismo que se encarga de la implantación de la ciberseguridad en los servicios públicos (detección y prevención de incidentes, labores de concienciación...), el fomento de la industria de la ciberseguridad, la I+D+I y el talento, ya que en la actualidad no se encuentran profesionales para cubrir plazas de este tipo; y el desarrollo de las tecnologías de ciberseguridad con la ayuda de la red nacional de laboratorios industriales, fabricantes, universidades, industrias de ciberseguridad y los usuarios finales. En su participación, explicó tres proyectos:

- ICS Arsenal: identificar las herramientas de ciberseguridad que están utilizando los malhechores para atacar las infraestructuras, centralizando todas las herramientas, recursos, simulaciones... y que los responsables de seguridad pueden utilizar en el momento que consideren.
- Escila: participación en proyectos europeos en las que las empresas se benefician de la financiación y conocimiento, elevar la ciberseguridad identificando problemas de ciberseguridad en forma remota .
- ICS SCAN: monitorización e identificación del nivel de exposición que tienen los sistemas en internet. Gracias al motor de inteligencia de INCIBE pueden detectar la vulnerabilidad de los sistemas expuestos y aconsejar como solucionarlo.

CIBERSEGURIDAD Y TELEGESTIÓN

María del Prado Torrecilla, responsable *Customer Technical Service & Product Manager* de Lacroix Sofrel España, abrió el segundo bloque de la jornada con su ponencia 'Ciberseguridad en la telegestión 4.0 del ciclo integral del agua: Ecosistema S4'. Señaló que las instalaciones del ciclo integral del agua se consideran infraestructuras críticas y, por ello, deben de estar permanentemente monitorizadas. En este sentido, la telegestión es una práctica imprescindible para el control eficiente de las instalaciones de agua.

» Las instalaciones del ciclo integral del agua son infraestructuras críticas que deben estar siempre monitorizadas. En este sentido, la telegestión es una práctica imprescindible para el control eficiente de esas instalaciones

Las comunicaciones son fundamentales para la telegestión. Estas han evolucionado mucho en los últimos tiempos, desde la telefonía fija (RTC) y radios analógicas hasta los soportes de comunicación basados en las comunicaciones IP (3GPP) que se han ido transformando en 2G, 3G, 4G y, actualmente, la 5G. También el IoT ha hecho surgir tecnologías LPWAn (LTE-M, NBioT, Lora, Sigfox) que obligan a desarrollar la ciberseguridad. Según la experta de Sofrel, para que un sistema sea ciberseguro es necesario un buen control de accesos, y se debe hacer una protección periférica de las comunicaciones. Existen varias soluciones: APN privadas suministrados por los operadores de telefonía, servidores VPN suministrando IP fijas seguras. Actualmente se protege el SCADA y las comunicaciones, pero no es habitual proteger los equipos instalados en campo. Es necesario garantizar la disponibilidad de los datos, la confidencialidad, la integridad, la autentificación y trazabilidad en los intercambios de datos en cualquier punto de la red.

Como solución, Lacroix Sofrel propone su ecosistema S4, compuesta por la estación remota Sofrel S4W y distintos *softwares* que garantizan la confidencialidad mediante certificados electrónicos estándares, la autentificación, la integridad de los datos mediante el servidor VPN SG4000 y su trazabilidad, compatible con protocolo Syslog para monitorizar todas las tramas relativas a la seguridad. Con esta solución "garantizamos la ciberseguridad dentro del núcleo de la solución, autentificamos protocolos seguros, ciframos las comunicaciones, la monitorización y los túneles VPN, y garantizamos la ciberseguridad".Finalizó su ponencia destacando que la transformación digital ha influido enormemente en el ciclo integral del agua y la telegestión es un elemento clave para poder garantizar una gestión inteligente de unas redes de agua.

Tras esta intervención fue el turno para Manel Escatllar, jefe del Departamento de Sistemas de Información del Consorci d'Aigües de Tarragona (CAT), y Jordi Jiménez, técnico de Telemando del CAT. El primero explicó la estructura de comunicaciones definida en la empresa, teniendo en cuenta su condición de suministradores de agua en alta a 63 ayuntamientos y 26 industrias, con más de 400 km de tubería, con 41 depósitos y 271 instalaciones relacionadas más entre bombeos y terciarias. En este sentido, la estructura de comunicaciones del CAT se divide entre fibra óptica para las instalaciones locales y diversos soportes para las instalaciones repartidas: radio, microondas, fibra óptica, cable, etc. La gestión de las comunicaciones se realiza mediante SCADA CITEC.

Por su parte, Jiménez expuso la experiencia del CAT integrando los equipos Sofrel. Ante la necesidad del Consorci de disponer de datos de caudal, nivel y presión, se requerían equipos que no tuvieran alimentación, que fueran fácilmente integrables en el sistema, con comunicación sin hilos 3G y datos que fueran fiables y seguros. Como solución optaron por LS Flow y LS42. Además, en los depósitos se optó por instalar LS42 y las informaciones se enviaban a estación remota S4W en el depósito que tiene el control del ramal y, de esta forma, poder hacer una regulación de la demanda. A nivel de seguridad, y por estar conforme con la ISO 270001 y seguridad en la comunicación 3G, se seleccionó un APN privada que permite diversas direcciones IP, con comunicaciones privadas y con un *router* 3G, dedicado en el que se concentran las informaciones de la red y se reciben en el SCADA. El resultado de implementar el telecontrol es la mejora de la información disponible en campo, la versatilidad que ofrecen los equipos Sofrel, la facilidad de integración en el SCADA, resultando un sistema seguro y robusto.

Finalmente, José Luis de las Cuevas, gerente de la empresa integradora ICR, describió en su ponencia 'La evolución e implementación de ciberseguridad en redes de hidráulicas' la migración de equipos Sofrel antiguos a las nuevas S4W por la necesidad de implementar ciberseguridad y nuevas tecnologías. Para ello se centró en dos casos específicos:

- Centro de control de regadío en Almería. En este caso, se instalaron estaciones remotas S500, con una red Wimax y red GPRS con un SCADA CITEC. De esta forma se paso de un sistema de comunicación tradicional con un cortafuegos a un sistema de ciberseguridad.
- Red hidráulica de la Costa Tropical en Granada. En este caso, esta zona compleja de montaña ya contaba desde 1999 con un primer telecontrol en la red de aguas, formado por 40 estaciones remotas S50 por RTC. Esta red se fue ampliando con remotas del tipo S500, hasta alcanzar las 22 unidades. El SCADA instala-

do era el Wizcom (control maestro). Pero la operadora de telefonía, en un momento dado, dejó de dar servicio, con lo que obligó a cambiar el sistema de comunicación al quedarse obsoleto. Con la última remodelación, se han sustituido 48 estaciones remotas S50 por las nuevas remotas S4W, se han modificado los cuadros, rehecho la programación y cambiado el tipo de comunicación de RTC a GPRS. Estos cambios han permitido aumentar el número de informaciones, la disponibilidad de estos datos de manera más rápida al tener comunicaciones GPRS/3G, con una configuración mucho más sencilla. Además, la estación remota S4W permite al integrador implementar de una manera sencilla, rápida y económica la ciberseguridad gracias a las herramientas que vienen ya de base.

CONCLUSIONES

Pese a los avances, las tecnologías relacionadas con la ciberseguridad en el ciclo del agua son tecnologías basadas en el *software,* por lo que tienen vulnerabilidades tanto conocidas como no conocidas, como por ejemplo atacar las redes con la pérdida del servicio o falsear los datos para causar daño. Por tanto, las redes de agua actualmente no son ciberseguras. Existen soluciones, como las de Sofrel, que permiten que las redes sean más ciberseguras, pero esa seguridad ya no es solo cuestión de tecnologías o cómo desplegarlas, sino que va más allá: se deben gestionar y mantener.

Por todo ello, tanto a nivel europeo como nacional se está trabajando para tener un sistema de certificación de tecnología a nivel de ciberseguridad, la normativa NIS. El organismo europeo que transpone esta normativa es ENISA y existe lo que se denomina Cybersecurity AT, un sistema que trabaja en esquemas de certificación de tecnologías que cumplen con requisitos de ciberseguridad. En España, el organismo es CN-CERC, que dispone de un esquema de evaluación de tecnología llamado LINCE. También en España, la normativa NIS transpuesta en el RD12/2018, regula y refuerza la seguridad de las redes y SI utilizados por los servicios esenciales, obligando al operador a notificar los incidentes en tiempo y forma. Pero deberá desarrollarse más para poder regular mejor los procesos.

En cualquier caso, y a la espera de unas normativas y certificaciones más específicas, es muy importante que las empresas operadora de agua dispongan de un análisis de evaluación de riesgos, protocolos y soluciones técnicas que ayuden a disminuir las vulnerabilidades en el ámbito de la seguridad cibernética, no solo por la propia seguridad de los datos con los que cuenta una empresa, sino también por la confianza que debe generarse hacia la ciudadanía, es decir, el cliente. Actualmente, los ataques son más sofisticados y el peligro ya no solo está en los datos del usuario, sino también en dejarlo sin agua.

En el mundo de la gestión inteligente del agua, cada vez más conectado, donde los puntos de acceso a los sistemas de gestión se multiplican, la ciberseguridad adquiere una importancia creciente. La mayor conciencia y el trabajo colectivo parecen ser el camino propuesto por las partes interesadas para construir un entorno más seguro. Sin lugar a duda, esta conferencia, que reunió a los principales actores públicos y privados en la gestión del agua junto con expertos institucionales en ciberseguridad, ha contribuido a cumplir este objetivo.