La seguridad inteligente en sistemas e instalaciones de agua

Tecnoaqua analiza los desafíos de la seguridad física, lógica y tecnológica para las empresas de suministro de agua

Rubén J. Vinagre, coordinador editorial de *Tecnoaqua*

La revista y portal *Tecnoaqua*, en colaboración con la Asociación Española de Abastecimientos de Agua y Saneamiento (AEAS), organizó el pasado 7 de junio en Madrid la jornada técnica 'Seguridad inteligente en sistemas e instalaciones de agua', cuyo objetivo fue analizar las obligaciones y necesidades actuales y futuras de seguridad en los servicios de abastecimiento y suministro de agua. La jornada a jornada se dividió en dos bloques. En el primero, expertos en seguridad de grandes operadores de agua mostraron sus planes de seguridad, a la vez que debatieron sobre hacia dónde se encamina la seguridad en las instalaciones de agua y cómo proteger las infraestructuras hidráulicas, incluyendo elementos de ciberseguridad. En un segundo bloque, fueron las empresas e ingenierías privadas las que explicaron su experiencia en la seguridad de sistemas e instalaciones de agua, desde varios puntos de vista o actuación: control de sensores y monitorización, infraestructuras de comunicación, gestión de datos del operador, nuevas tecnologías (*big data*, industria 4.0), ciberseguridad, etc. La jornada contó con el patrocinio de las siguientes empresas: Everis, Global Omnium, Indra y Lacroix Sofrel.

El Plan Nacional de Protección de las Infraestructuras Críticas establece como infraestructuras críticas aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos. Entre ellas se incluyen las infraestructuras relacionadas con el suministro de agua, como los embalses, las instalaciones de almacenamiento, las plantas de tratamiento y las redes de abastecimiento de agua. El criterio para considerar crítica a una infraestructura es una mezcla de factores (rango, escala y efectos en el tiempo) y de parámetros (daños causados, impacto económico e impacto en servicios esenciales).

Si bien dicho plan está planteado como respuesta al riego de "ataques terroristas catastróficos" contra infraestructuras críticas, no es difícil pensar que el agua puede ser un objetivo para todos aquellos que quieran desestabilizar una sociedad sin alcanzar tal magnitud. Las infraestructuras también pueden ser objeto de sabotajes, ciberataques contra los sistemas informatizados o, incluso, contra la protección de datos de los usuarios de las compañías gestoras. Actualmente, son las instalaciones de agua de las grandes ciudades las que se incluyen en la lista de infraestructuras críticas y, por tanto, las que están obligadas a tener un plan específico de seguridad. No obstante, para los responsables políticos las instalaciones de sus municipios, sean estos medianos o pequeños, son tan prioritarias como las otras. Ante esta necesidad, y también porque el nivel de 'criticidad' debe ir a la baja, es imprescindible conocer qué debe incluir un plan específico de seguridad, qué infraestructuras se deben priorizar para evitar fallos en los sistemas, qué protocolos y procedimientos seguir, cómo avisar a los ciudadanos, cuándo restaurar el servicio, etc.

Para dar respuesta a todo ello, *Tecnoaqua*, en colaboración con AEAS, organizó la jornada técnica 'Seguridad inteligente en sistemas e instalaciones de agua', con la idea de facilitar la mayor información posible a todas las empresas de agua que, con servicios de captación, tratamiento, almacenamiento y distribución, tengan a corto, medio o largo plazo que adoptar unas medidas de seguridad sin ser traumático ni para la organización ni para los usuarios.

LA SEGURIDAD EN EL SECTOR DEL AGUA

Como explicó Fernando Morcillo, presidente de AEAS en la inauguración de la jornada, el sector del agua siempre ha tenido presente la seguridad, pero tradicionalmente se ha centrado en la seguridad operativa y laboral.

Momento de la inauguración de la jornada, con Fernando Morcillo, presidente de AEAS.

Aunque son muchos los antecedentes históricos sobre la seguridad en tiempos de guerra, la humanidad siempre ha tenido un cierto grado de moralidad sobre el abastecimiento de aguas a la población, siendo notorio que salvo contadas ocasiones se ha controlado el abastecimiento para reforzar los asedios militares. Hoy, la tensión terrorista ha cambiado el paradigma, y por ello no solo hay que atender la *safety*, sino también la *security* (técnicas mucho más novedosas y menos conocidas y tradicionales en el sector).

Tras los atentados de principios de siglo hay una corriente a nivel mundial, liderada por los países más desarrollados, para fijar estrategias de prevención y protección. Esta tendencia se extiende rápidamente a la ciberseguridad, dado el grado de posibles incidencias sobre las comunicaciones, los sistemas informáticos, automáticos o telemáticos.

A nivel legislativo, Europa toma conciencia de ello sobre todo en 2004, cuando el Consejo Europeo insta a la Comisión Europea a elaborar una Estrategia sobre Protección de Infraestructuras Críticas, aprobándose el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) y la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN).

En España, todo ello llega tres años más tarde, en 2007, con el Primer Plan Nacional de Protección de Infraestructuras Críticas, el Catálogo Nacional de Infraestructuras Estratégicas y el Acuerdo sobre Protección de Infraestructuras Críticas. Desde entonces, se han dado avances como la aprobación de la Unión Europea a la Directiva 2008/114 y su trasposición al ordenamiento jurídico español como Real Decreto 3/2010 Esquema

Nacional de Seguridad, la Ley 8/2011 por la que se establecen medidas para la protección de infraestructuras críticas, como la creación del CNPIC, o el Reglamento 704/2011 de Protección de Infraestructuras Críticas.

Pero no es hasta 2013 cuando se establecen las reglas generales en relación con la ciberseguridad con la presentación de la Estrategia de Ciberseguridad de la Unión Europea, el Reglamento GDPR, la Ley 40/2015 de Régimen Jurídico del Sector Público y la Directiva 2016/1148 para garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea.

El sector, a través de AEAS, tomó en consideración la legislación española y ha venido apoyando al CNPIC en materia técnica y divulgativa y creando un Grupo de Trabajo de Operadores Críticos que se traslada a los asociados expertos la información oficial producida por diferentes entidades administrativas del Estado.

LA EXPERIENCIA DE LOS GRANDES OPERADORES

El bloque de experiencias de los grandes operadores de agua lo inició Javier Marino, director de Seguridad del Canal de Isabel II, quien explicó la situación de la seguridad física y lógica en el Canal de Isabel II, las amenazas y paradigma de las infraestructuras críticas y la evolución que la empresa ha llevado a cabo para implantar nuevas soluciones y medidas en seguridad. Como resumen, señalar que mantener la seguridad no es fácil, pues las nuevas amenazas son más difusas, capaces y fuertes. Existe una evolución de la seguridad de reactiva a proactiva y no se debe descuidar que siguen existiendo los riesgos clásicos. Por ello, es fundamental el conocimiento y empleo de todas las capacidades y tecnologías (multidisciplinar) y es necesaria la especialización y profesionalización de la seguridad, implicando a toda la empresa y su personal. La seguridad es integral, global y permanente.

Los grandes operadores de agua (Canal de Isabel II, Global Omnium, Suez...) explicaron sus experiencias en seguridad.

Seguidamente, José Miguel Silva Pérez, vocal del Grupo Intrasectorial de Seguridad en Servicios del Agua de AEAS y de Acosol, ofreció una visión evolutiva desde AEAS. Según Silva, no se puede dividir la seguridad en un mundo interconectado, no solo por la interconexión de sistemas en red y movilidad, que engloban el concepto de ciberseguridad, sino porque las seguridad viene íntimamente unida a la interdependencia del acceso, prudencia y confidencialidad en el manejo de información, a la ética personal y corporativa de los empleados, proveedores y de los clientes, a los procedimientos conectados con la criminalidad y la responsabilidad civil, con seguridad y salud laborales, al diseño de las instalaciones, e incluso a los procedimientos productivos. La calificación de las empresas por criticidad ha servido fundamentalmente para concienciar a un sector que culturalmente estaba muy desconectado de la seguridad. El objetivo es la búsqueda de la seguridad total.

En su turno, Herminio Noguera Ruiz, responsable SOC 360 - Seguridad Integral, de la Dirección de Seguridad Corporativa de Suez Spain, explicó el modelo de convergencia en la gestión técnica de la seguridad integral en su compañía, basado en el análisis de la convergencia en la gestión técnica de la seguridad en todas sus vertientes como modelo de seguridad integral, y del control operativo de plataformas, gestión y tratamiento de eventos, indicadores y análisis de amenazas.

Para finalizar este bloque, José Luis Delgado, responsable de Seguridad y Enlace de Emivasa, ofreció también una visión integral de la seguridad. En su opinión, la seguridad ha sido y es una asignatura pendiente en la marcha parte de las empresas dedicadas a la gestión de los servicios públicos, no tanto por los medios que han destinado tradicionalmente a tal fin, sino por la falta de percepción real del riesgo dentro de la organización, en muchos casos ajena totalmente a la realidad social y a la creciente preocupación en esta materia. En los últimos años, motivado fundamentalmente por el *expertise* adquirido en materia de gestión de riesgos, las empresas de Global Omnium han liderado sectorialmente la consecución de determinados hitos y acontecimientos en materia de gestión de riesgos y seguridad: primera empresa certificada en Europa de cualquier sector en materia de gestión de riesgos (2013); primera empresa certificada en el sector en España en materia de gestión de activos (2017); y primera empresa certificada en el sector en Europa en materia de respuesta ante emergencias (2018).

Representantes de las empresas Lacroix Sofrel, Everis, Indra y Global Omnium mostraron sus distintas soluciones de seguridad para el sector del agua en el segundo bloque de la jornada de *Tecnoaqua*.

SOLUCIONES EN SEGURIDAD

En el bloque de soluciones, María Taberna, directora de Ciberseguridad Industrial IoT de Oylo Trust Engineering, explicó la estrategia de protección y resiliencia para infraestructuras críticas adaptada a las nuevas tecnologías y basada en *data-decision-driven* asociado al proceso crítico de negocio.

Desde Lacroix Sofrel, María del Prado Torrecilla, responsable Customer Service & Formación y jefa de Producto, analizó la evolución de las tecnologías de comunicación, las soluciones para responder a las necesidades del Internet of Things (IoT), la repercusión en materia de seguridad (ciberseguridad), todos los aspectos a tener en cuenta y, por último, cómo responde Lacroix Sofrel a estas nuevas exigencias a través de su ecosistema de telegestión Sofrel 4 Water (S4W): una solución diseñada para responder a las nuevas necesidades de los explotadores de agua que permite garantizar un alto nivel de protección y de seguridad y facilitar de esta forma la gestión de las redes de telegestión conectadas permanentemente.

Precisamente, ante la creciente necesidad de analizar los mecanismos de seguridad de infraestructuras críticas de agua, Everis Ingeniería ha desarrollado Swalert, un sistema de monitorización y protección de las infraestructuras críticas de abastecimiento de agua que detecta, mediante el análisis en tiempo real de la huella fisicoquímica de un conjunto de parámetros, las variaciones en la calidad del agua provocadas por la presencia de contaminantes. En este contexto, Pedro Peñalver Martínez, director del Área de Agua de Everis Ingeniería, analizó durante su intervención la situación actual en materia de protección de redes de abastecimiento y los últimos avances en la implementación de medidas de protección en sistemas de distribución de agua potable. Así, Swalert es una herramienta que supone un importante avance en la implantación de tecnología aplicada al campo de la alerta temprana en el suministro de agua urbana. Además, según Peñalver, en los tiempos que corren es importante poner el foco de atención en la protección de las infraestructuras de agua puesto que la vulneración de las mismas afecta directamente al elemento más sensible del sistema, que es la confianza del usuario en el suministro seguro. Una vez perdida esta confianza es muy difícil de recuperar, y requerirá de medidas activas, lentas y de alto coste.

Desde Indra, su director de Energy&Utilities Maurizio De Stefano, explicó que la transformación digital de las *utilities* de agua y la introducción de las nuevas tecnologías, como por ejemplo el IoT, estarán cada vez más presentes en el mundo del agua y, aunque esto es fundamental para mejorar la gestión, también hay que tener cuidado porque en un futuro no muy lejano (si es que no está pasando ya) la mayor parte de las amena-

Principales Impactos provocados por amenazas en el sector del agua y sus infraestructuras (IT y OT).

zas que hayan de afrontar las infraestructuras críticas provendrán de dispositivos conectados a Internet, pudiéndose el sector del agua convertirse en un blanco ideal para ataques terroristas. Según datos aportados, el CERT-SI gestionó durante el año 2016 en España casi 110.000 incidentes de los que 146 iban dirigidos a infraestructuras críticas, el doble que el año anterior. En Estados Unidos, sobre el sector del agua recayó el cuarto mayor número de incidentes en ciberataques, el tercero si se tienen en cuenta también los ciberataques a presas hidráulicas. Por el contrario, se estima en los próximos 5 años el cibercrimen causará unas pérdidas de 8 trillones de dólares. Las empresas del sector de energía y *utilities* dedican de media a ciberseguridad un 4% de su presupuesto de TI. Esto es insuficiente frente a la creciente interconexión y automatización de sus redes y ataques, cada vez más sofisticados. Y solo el 54% de las *utilities* tienen un programa para inventariar y proteger sus activos de información sensibles.

Por último, Juan Luis Pozo, CISO y director del Área de Sostenibilidad Corporativa de Global Omnium, habló sobre la inteligencia en la respuesta de emergencias. Según este experto, los servicios públicos se encuentran abocados, para asegurar su garantía total de continuidad ante cualquier contingencia, a incluir la ciberseguridad como una de sus primeras prioridades, pues la transformación digital de la sociedad ha modificado considerablemente la capacidad de respuesta y la resiliencia ante la contingencia. La respuesta ante cualquier emergencia ha evolucionado de forma muy positiva gracias a las tecnologías y a la transformación digital, que han permitido una mayor interacción entre los ciudadanos en general y los usuarios de los servicios públicos en particular, pero al mismo tiempo no es ajena en modo alguno al nuevo y principal reto del siglo XXI, la veracidad e integridad de la información necesaria para los procesos de toma de decisiones. En este nuevo marco la inteligencia artificial ha pasado de jugar un papel de actor secundario en cuanto a ser una herramienta de test de vulnerabilidad a convertirse en el actor principal de la actuación, pues en aras a evitar el error humano las empresas se dotan de un modelo de inteligencia artificial que evoluciona vertiginosamente y que permite una mayor capacidad de resolución de situaciones, pero al mismo tiempo genera un nuevo riesgo tal cual es la dependencia tecnológica de unas herramientas que podrían estar siendo *hackeadas*. En el caso de Global Omnium está inteligencia se demuestra con la implantación de CiberSOC, una herramienta de seguridad, detección y prevención de ciberataques que realiza continuas simulaciones de la capacidad de respuesta ante cualquier contingencia.

CONCLUSIONES

La seguridad es un elemento trascendente para asegurar la continuidad y resiliencia de los servicios urbanos

del agua. Siguiendo la metodología y el ejemplo de los grandes operadores de infraestructuras críticas, los servicios de poblaciones más pequeñas deben establecer sus programas y planes sobre seguridad de sus sistemas. Es fundamental que todas las empresas, indistintamente de su tamaño, adopten unas medidas y planes de seguridad (física, lógica, industrial, tecnológica, ciberseguridad...) e inviertan en ellos.

Muchas de estas medidas pasan por implementar nuevas soluciones, como el empleo de drones, el desarrollo de sistemas de alimentación sostenibles y seguros, sistemas cierre y endurecimiento de parámetros y cerramientos o incorporar sensores y analizadores de ultima tecnología.

No obstante, los retos de la seguridad integral del sector del agua, más allá de aplicar nuevas tecnologías, sistemas y soluciones TIC, también requieren un cambio cultural, en consonancia con los nuevos tiempos. Hay que saber, por ejemplo, que la gestión del miedo está vinculado con la generación de confianza. En un mundo donde las noticias 'vuelan' a través de los medios y las redes sociales, es prioritario educar en la concienciación y la ética y no participar en la sociedad del odio y del escándalo.

Lógicamente, hay que estar atentos a la ciberseguridad, pues son ataques que invalidan la producción y potencias los robos de datos. Hay que proteger todas las redes, las físicas pero también las esencias y las estratégicas. Las empresas, no solo deben cumplir con la normativas, sus objetivos y plazos (gestión multirriesgo), sino también apostar por la transversalidad: seguridad privada, ley de protección de datos, *legal compliance*, RRLL operativos, evacuación...

Para una buena seguridad es necesaria la profesionalización interna y la coordinación externa, una gestión centralizada y la capacidad de gestión multirriesgo y multievento y, sobre todo, una gran capacidad de respuesta.