PERSPECTIVAS IMTA
N°. 13, 2021
Autor: Laurent Courty
DOI: doi.org/10.24850/b-imta-perspectivas-2021-13

Los retos de la seguridad informática en la digitalización del agua

Autor:
Laurent Courty
Fecha de publicación:
14 de marzo de 2021

Además de la disrupción de la operación de los sistemas de aguas, los ciberataques pueden usarse también para realizar fraudes.

Si bien las ventajas de la digitalización del agua son numerosas, eventos recientes nos recuerdan la importancia de establecer protocolos de seguridad adecuados para mantener la calidad del servicio y la salud de la población.

Los retos del cambio climático, combinados con los de la urbanización, hacen esencial el uso de soluciones computarizadas para el monitoreo, la operación y el mantenimiento de las variables del ciclo hidrológico urbano [1]. Sin embargo, ataques recientes a plantas potabilizadoras han mostrado la vulnerabilidad de los sistemas de agua ante ataques informáticos, un problema exacerbado por el desarrollo del internet de las cosas (IoT, por su sigla en inglés). Este término se refiere a la conexión directa a internet de pequeños aparatos autónomos, en contraste con los dispositivos operados directamente por humanos, cómo un teléfono o una computadora. En la vida diaria, una multitud de aparatos tienen ahora una versión "conectada", por ejemplo, una lavadora, una cafetera, un videoportero y hasta un dispensador de alimentos para mascotas. La misma tendencia a los dispositivos conectados se observa en la industria, y la gestión del agua no es la excepción.

En 2020 se sospechó que actores gubernamentales de Irán habían infiltrado los sistemas informáticos de empresas de agua de Israel para subir el nivel de cloro en el agua distribuida a la población [2]. En un

Autor: Laurent Courty
DOI: doi.org/10.24850/b-imta-perspectivas-2021-13

caso similar, y más mediatizado, la planta potabilizadora de Oldsmar en Florida sufrió un ciberataque en febrero de 2021 que multiplicó por más de 100 veces el nivel de sosa caustica utilizada en el tratamiento del agua [3]. Si el personal de la planta no se hubiera percatado de la modificación, miles de usuarios hubieran recibido agua peligrosa para su salud. En abril de 2021 se dio a conocer que un exempleado de una potabilizadora en Kansas se conectó de manera remota al sistema informático de la planta y procedió a apagar los trenes de tratamiento [4]. Estos sucesos tienen en común que son ataques remotos a plantas que producen agua potable para el consumo humano, con el fin de modificar el proceso de tratamiento y dañar así la salud de los usuarios. Estos ataques se realizaron mediante la conexión remota a los sistemas de supervisión, control y adquisición de datos (Scada por sus siglas en inglés) que ayudan al personal a operar las plantas.

Si bien es cierto que los sistemas Scada se han usado en la operación de sistemas de agua durante décadas, estos eventos recientes son un recordatorio de la necesidad te tomar en cuenta de manera seria la seguridad informática en el diseño y operación de las redes de aguas y servicios afines. Esta amenaza se vuelve aún más aguda por la multiplicación de aparatos conectados de tipo IoT, un tema bien identificado por la comunidad científica [5]. Personas malintencionadas pueden atacar las redes de IoT de manera general, por ejemplo, establecer un botnet vía software tipo Mirai [6], o de manera puntual, apuntando a las funciones específicas del equipo. Por ejemplo, modificar la lectura de un sensor de nivel en un cárcamo de bombeo puede detener el bombeo y causar problemas de abastecimiento.
Además de la disrupción de la operación de los sistemas de aguas, los ciberataques pueden usarse también para realizar fraudes. Por ejemplo, la norma NMX-AA-179-SCFI-2018 para la medición de aguas nacionales se basa en la tecnología IoT, con transmisión diaria de datos a la Conagua. Su puesta en marcha [7] será sin duda un gran avance para mejorar el control de las concesiones de aguas nacionales y limitar el acaparamiento ilegal del agua; sin embargo, es necesario tener cuidado en su implementación para limitar los vectores de ataque, notablemente para evitar la transmisión de datos por el protocolo obsoleto y vulnerable FTP [8].

La seguridad de los sistemas de información en general, y de las redes IoT en específico, es un tema complejo que nosotros, los profesionales del agua, no podemos pretender comprender en su totalidad. Es tiempo de que nuestro sector tome más en serio esta temática y colabore de manera más cercana con expertos en la materia, para asegurar así el monitoreo y la operación fiel y segura de la infraestructura hidráulica.

[1] Pedrozo-Acuña, A. (2020) Agua inteligente, ciudades inteligentes. https://www.gob.mx/imta/es/articulos/agua-inteligente-ciudades-inteligentes?idiom=es

[2] https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/

[3] https://edition.cnn.com/2021/02/11/us/florida-water-plant-hack/index.html

[4] https://arstechnica.com/information-technology/2021/04/man-indicted-for-allegedly-tampering-with-computer-at-public-water-plant/

[5] Noor, M. M., Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294. https://doi.org/10.1016/j.comnet.2018.11.025.

[6] https://en.wikipedia.org/wiki/Mirai_(malware)

Autor: Laurent Courty
DOI: doi.org/10.24850/b-imta-perspectivas-2021-13

[7]Acuerdo por el cual se reforma el artículo segundo transitorio de las Reglas Generales sobre Medición de Aguas Nacionales a que se refiere la fracción I, del párrafo tercero, del artículo 225, de la Ley Federal de Derechos. DOF: 19/05/2020

[8] http://mywiki.wooledge.org/FtpMustDie