¿Se puede hackear la cadena de frío? Un ciberataque puede alterar temperaturas y alarmas

- *Los ataques registrados en supermercados de Bélgica y Suecia muestran que la conectividad de los sistemas de refrigeración también puede abrir nuevas vulnerabilidades. Especialista UCSC explica qué ocurre cuando alguien accede a sus controles.*

Un refrigerador industrial ya no es solamente un equipo que produce frío: también puede estar conectado a redes informáticas que permiten supervisarlo y controlarlo a distancia. Esa capacidad facilita su operación y mantenimiento, pero también abre una puerta inesperada: si alguien logra acceder sin autorización, podría modificar temperaturas, presiones o ciclos de deshielo y comprometer toda una cadena de frío.

El escenario quedó en evidencia tras los ciberataques registrados en sistemas de refrigeración de supermercados de Bélgica y Suecia. Para Carlos Salinas, Jefe de carrera de Técnico Universitario en Refrigeración y Climatización Industrial del Instituto Tecnológico de la Universidad Católica de la Santísima Concepción (UCSC), estos casos muestran los riesgos asociados a la creciente conexión de este tipo de infraestructura.

“Un acceso no autorizado a los sistemas de control, como PLC y plataformas SCADA, podría permitir la alteración de parámetros críticos, como temperaturas, presiones y ciclos de deshielo, comprometiendo la conservación de los productos, la integridad de los equipos y la continuidad operacional, con eventuales

consecuencias económicas y sanitarias”, explicó.

¿Qué ocurre si nadie detecta la intervención?

El principal problema aparece cuando la manipulación pasa inadvertida y el sistema continúa operando bajo parámetros incorrectos.

Según Salinas, una de las primeras consecuencias puede ser la pérdida de la cadena de frío, provocando el deterioro de alimentos y el eventual descarte de productos. A ello se suma el riesgo para la propia infraestructura. Una operación fuera de los rangos normales puede afectar compresores, evaporadores y otros sistemas auxiliares.

El problema puede ser todavía más difícil de identificar si el ataque modifica los mecanismos encargados de advertir una anomalía.

“Puede producirse una disminución de la confiabilidad operacional, producto de la alteración de registros de temperatura, la desactivación de alarmas o la entrega de información falsa que dificulte detectar oportunamente el problema”, señaló el Jefe de carrera.

Más conectividad también exige más protección

Frente a estas vulnerabilidades, la seguridad de un sistema de refrigeración industrial ya no depende únicamente de su funcionamiento mecánico o eléctrico. También requiere proteger los sistemas digitales encargados de supervisarlo y controlarlo. Entre las principales medidas, Carlos Salinas identifica la segmentación de las redes de control y la separación entre las redes administrativas y aquellas vinculadas directamente con los procesos industriales.

Los accesos remotos, además, deben contar con autenticación multifactor y permisos restringidos, evitando que cualquier usuario pueda modificar parámetros críticos.

“También es fundamental establecer rangos autorizados para las temperaturas y otros parámetros críticos, implementar sistemas independientes de monitoreo y alarmas, mantener protecciones físicas y eléctricas que funcionen incluso ante fallas de supervisión y contar con planes de mantenimiento y contingencia”, explicó el docente del Instituto Tecnológico UCSC.

Los casos registrados en Europa muestran así un nuevo desafío para instalaciones que dependen de la refrigeración continua: mientras más conectados se encuentran sus sistemas de control, más importante resulta integrar la ciberseguridad a la operación cotidiana para evitar que una intervención digital termine provocando consecuencias físicas sobre equipos, productos y procesos.