Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Fatality File – Spanish



Un hacker obtiene acceso remoto a una planta de tratamiento de agua en Florida e intenta envenenar el suministro de agua de 15 000 residentes manipulando los sistemas de control químico

Qué Sucedió

El 5 de febrero de 2021, un hacker no autorizado obtuvo acceso remoto a la planta de tratamiento de agua Bruce T. Haddock en Oldsmar, Florida, utilizando TeamViewer –una aplicación de escritorio remoto que compartían todos los empleados de la planta con una sola contraseña y sin ningún firewall instalado–. El atacante accedió al sistema SCADA de la instalación y modificó la concentración de hidróxido de sodio de 100 partes por millón a 11 100 partes por millón –un nivel capaz de causar quemaduras químicas graves o la muerte si llegara a los consumidores–. Un operador de la planta, que se encontraba alerta, notó que el cursor se movía en su pantalla, observó en vivo cómo el atacante navegaba por el sistema e inmediatamente revirtió el cambio antes de que pudiera surtir efecto.

¿Qué Salió Mal?

La investigación reveló que los empleados habían estado utilizando una versión de Windows sin soporte técnico y sin firewall, y que compartían una única contraseña de TeamViewer entre todo el personal, lo que le daba a cualquier actor externo que obtuviera la contraseña control total y en tiempo real sobre un proceso químico crítico para la seguridad. No existía autenticación multifactorial. Ningún sistema de detección de anomalías alertó sobre el acceso no autorizado. La única barrera entre una fuga química letal y 15 000 residentes fue un trabajador que observaba su pantalla en el momento adecuado.

Conclusión

Este incidente se detuvo gracias a la atención humana, no a los sistemas diseñados para monitorear y controlar la planta. Cada sistema de seguridad conectado es tan seguro como su punto de acceso más débil, y cada lectura de un sensor es tan confiable como el sistema que la reporta. Los trabajadores deben saber lo que sus sistemas digitales no pueden detectar y estar preparados para verificar las condiciones de manera independiente.

Fuente: Securitymagazine.com