

LA ÚNICA RESPUESTA VÁLIDA PARA HACER FRENTE A LOS CIBERATAQUES

CIBERSEGURIDAD: GARANTIZA EL FUTURO DE TU ESTACIÓN DE SERVICIO

Mezclar gasolina, agua y diésel, modificar los precios del combustible, generar vertidos incontrolados, alterar la información relativa al número de litros de combustible almacenados o dispensados, o provocar explosiones son algunas de las desastrosas consecuencias de un posible ciberataque en una estación de servicio.

Luis Ángel Martínez,
director de Sistemas y
Ciberseguridad de Proconsi



Hace unos meses supimos de la existencia de una serie de ciberataques contra los sistemas de pago de varias estaciones de servicio en Estados Unidos. El objetivo de estos ataques era acceder a los datos de las tarjetas de crédito empleadas por los clientes para realizar los pagos de las recargas de combustible, aprovechando para ello una vulnerabilidad generada por una tecnología obsoleta.

El proceso de digitalización de las empresas industriales está en pleno auge. La inclusión de nuevos sistemas de automatización y tecnologías inteligentes implica ventajas sustanciales

en lo que al proceso productivo y de gestión se refiere. Sin embargo, también propicia la aparición de nuevas amenazas ante las que estar protegido mediante la inclusión de tecnologías actualizadas de detección, defensa y recuperación, es fundamental.

El número de ciberataques contra empresas dedicadas al sector de los hidrocarburos ha crecido de forma significativa durante los últimos años. El teletrabajo y la aparición de nuevos ataques más específicos y dirigidos han provocado la aparición habitual de noticias relacionadas con ciberataques a grandes petroleras, eléctricas y, cómo no, estaciones de servicio.

Luis Ángel Martínez, director de Sistemas y Ciberseguridad (CISO, en sus siglas en inglés) de Proconsi, apunta que "hace un par de años supimos de una alerta de seguridad que advertía de la existencia de más de un centenar de estaciones de servicio en riesgo elevado de ciberataque. En este caso concreto, la solución pasaba por un proceso tan sencillo como incluir una contraseña de acceso a los depósitos, algo que a posteriori nos parece una obviedad, pero que, en ese momento, debido a la falta de una buena configuración de los sistemas y una correcta formación de los equipos técnicos en temas de ciberseguridad, pudo resultar desastroso".

La inclusión de nuevos sistemas de automatización y tecnologías inteligentes implica ventajas sustanciales en lo que al proceso productivo y de gestión se refiere

En ocasiones el problema estriba en el hardware empleado, con deficiencias en su fabricación. En otras, son los sistemas informáticos los que fallan. Sin embargo, no podemos olvidar que en la mayor parte de los casos el factor humano es el más vulnerable.

En el año 2019, la petrolera mexicana Pemex sufrió un ciberataque que, según declaraciones de la propia compañía, afectó a un 5% de sus equipos. Las incidencias relacionadas con la ciberseguridad no es solo una cuestión de grandes corporaciones extranjeras. De hecho, según un informe reciente de la multinacional de ciberseguridad Kaspersky, las estaciones de servicio vulnerables se ubican en países como India, Chile, Estados Unidos, Turquía, Israel, Singapur y, por desgracia, España.

Hace un par de años, cinco personas robaron 120.000 litros de combustible en dos gasolineras de la periferia de París mediante un acceso remoto, poniendo las bombas en modo mantenimiento y, de este modo, extrayendo el combustible sin el control del contador. Meses después, una gasolinera de Detroit, Michigan, en Estados Unidos, dispensó gasolina gratis durante una hora y media a sus clientes debido al uso de un dispositivo que permitió a los atacantes bloquear en remoto el control de la bomba por parte del operario.



Proconsi cuenta el primer Centro de Operaciones en Ciberseguridad para Pymes de nuestro país.

proconsi

El número de ciberataques contra empresas dedicadas al sector de los hidrocarburos ha crecido de forma significativa durante los últimos años

Según declara el director de Sistemas y Ciberseguridad de Proconsi, "llevamos años protegiendo a nuestros clientes frente a todo tipo de ciberataques. En este tiempo hemos prevenido y solventado ataques que, de no contar con nuestros servicios, hubiesen generado problemas, como el apagado de los sistemas de abastecimiento, fugas de combustible, acceso a la información de los clientes, alteración de la identidades y matrículas de los conductores, accesos a los terminales de pago o cambio en los precios del combustible. Además, hemos facilitado a nuestros clientes servicios de recuperación de la información en aquellos casos en los que estos no contaban con un servicio de copia en la nube y habían sufrido un ataque de cifrado de su información; hemos afrontado intentos de suplantación de identidad, fraude al CEO, ataques de denegación de servicio, etcétera".

Servicios de seguridad gestionadas 24/7; auditorías de seguridad de la información, incluyendo auditorías de caja gris, caja negra y de cumplimiento de la RGPD y la LOPDGGD; análisis de vulnerabilidades web; 'backup online'; servicios de delegado de protección de datos o consultoría tecnológica para la implantación de un Sistema de Gestión de la Seguridad de la Información, conforme a la ISO 27001; de un Sistema de Gestión de la Seguridad de la Información, conforme al Esquema Nacional de Seguridad para la obtención del Sello de Ciberseguridad de la AEI o para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) son algunos de los muchos servicios de ciberseguridad que ofrece la tecnológica Proconsi, desde su SOC, el primer Centro de Operaciones en Ciberseguridad para Pymes de nuestro país. ■