¿Pueden los Hackers producir un apagón eléctrico?

Desde hace mucho tiempo, los expertos en seguridad de sistemas han advertido sobre la amenaza que hoy por hoy representan los piratas informáticos a los sistemas que ayudan a controlar las centrales las eléctricas, plantas de tratamiento de agua y los sistemas de transporte de los cuales dependen muchas personas en el mundo entero.

Justo antes de las pasadas Navidades, esa amenaza “teórica” se convirtió en una aterradora realidad para más de 225.000 ciudadanos ucranianos que quedaron totalmente a oscuras por un sofisticado ataque a una de las empresas de energía eléctrica de la nación.

La preocupante vulnerabilidad de las centrales nucleares a los ataques informáticos

Los hackers protagonistas del ataque, actuaron a última hora de la tarde el pasado 23 de diciembre 2015 utilizando el acceso remoto de los ordenadores en del centro de control de la planta Prykarpattyaoblenergo, bajaron todos los interruptores automáticos y apagaron también todas las subestaciones del complejo.

En total, fueron alrededor de unas 30 subestaciones las apagadas, incluidas aquellas que alimentan las salas de control de Prykarpattyaoblenergo, por lo que el personal que intentaba recuperar el servicio de la luz se vio obligado a buscar soluciones literalmente en la oscuridad.

Incluso hasta ahora, varios meses después del ataque, los sistemas informáticos de la empresa de energía de Ucrania no están al 100% debido a que el malware Killdisk, el cual fue utilizado en el ataque eliminó muchos archivos clave.

Defensas digitales contra Hackers

“La mayor vulnerabilidad se produce al conectar los sistemas informáticos con poca protección de la empresa a las tecnologías operacionales que son la columna vertebral de la misma”, afirmó el portavoz de la GCHQ.

“La gran mayoría de los ataques tienen primero como blanco a los sistemas informáticos de la empresa para luego actuar como si se tratara de un usuario legítimo para lograr que el ICS o OT haga algo”, añadió el vocero de la GCHQ.

“Existen buenas razones por las cuales los atacantes eligen esta vía”. “Es mucho más fácil explotar la empresa porque hay muchas herramientas que puede descargar y utilizar para hacer eso”, indicó el encargado de los sistemas de la planta eléctrica afectada.

Una empresa con optimas defensas contra las amenazas informáticas dirigidos a sus sistemas corporativos también ayudará a derrotar los intentos de subvertir esa o cualquier otra planta operada por medio de control remoto.

fuente:tecnomagazine