NINGÚN CUIDADO ES SUFICIENTE

Los problemas de ciberseguridad en la industria nuclear

El número de computadoras que las personas utilizan y con las que interactúan aumenta cada año, con el consiguiente incremento de las oportunidades de perpetrar ciberataques. (Fotografía: istockphoto.com)

El número de computadoras que las personas utilizan y con las que interactúan aumenta cada año, con el consiguiente incremento de las oportunidades de perpetrar ciberataques. Por ejemplo, los automóviles actuales contienen no menos de 12 canales digitales de entrada/salida para controlar el motor, la transmisión, la radio, el sistema de frenado antibloqueo, el sistema de apertura sin llave, el dispositivo antirrobo, el sistema telemático, etc. Todos estos sistemas tienen puntos vulnerables que pueden sufrir ataques.

La tecnología computacional y de la información evoluciona muy rápidamente y en ocasiones no nos da tiempo a conocer las posibles fuentes de cibervulnerabilidad y las modalidades de ataque más sofisticadas. Además, los ciberataques no se limitan al lugar de trabajo: también pueden perturbar la vida privada de las personas.

Uno de los principales objetivos de la labor que lleva a cabo el OIEA para mejorar la ciberseguridad es reforzar la cultura de la seguridad física nuclear para cambiar tanto la manera de pensar de las personas como la forma en que evalúan la adopción de la tecnología y su utilización.

"Si los profesionales del sector nuclear y sus familias cobran más conciencia no solo de su espacio físico sino también de su espacio digital serán más prudentes con respecto al intercambio de información en línea y el uso de la tecnología. Una información aparentemente inocua se puede combinar con otra información obtenida de alguna otra fuente en línea y puede resultar muy dañina. Google y otros motores de búsqueda por Internet suelen ser los primeros instrumentos que utilizan los piratas informáticos para elaborar un plan de ataque," dice el Sr. Dudenhoeffer.

Ben Govers, Coordinador nacional en materia de antiterrorismo y seguridad del Ministerio de Seguridad y Justicia de los Países Bajos, dice que poco a poco el reconocimiento de la importancia de esta amenaza está ganando terreno en la industria nuclear. "La industria nuclear debe afrontar el desafío de ampliar y al mismo tiempo profundizar sus actuales defensas contra las ciberamenazas en las redes computacionales y de información. La industria está empezando –en mayor o menor grado– a elaborar, aplicar y ampliar medidas enérgicas para proteger los sistemas de información y control de las instalaciones nucleares".

"Se trata de un proceso dinámico en el que el OIEA puede desempeñar una función destacada," dice el Sr. Govers.

Una comunidad de colaboradores

El virus informático Red October se descubrió en octubre de 2012. Se estima que durante un período de hasta cinco años permitió obtener información sensible en más de 60 países sin ser detectado. La información extraída de las redes infectadas podría volver a utilizarse en futuros ciberataques. El grado de sofisticación en

la ciberdelincuencia es cada vez mayor y representa un desafío adicional que el personal de seguridad nuclear debe afrontar.

El OIEA apoya en todos los niveles la labor que llevan a cabo los Estados encaminada a establecer programas sólidos y comprobados de seguridad computacional y de la información. Organiza programas regionales de capacitación, crea cursos para profesionales en seguridad física nuclear, publica directrices sobre ciberseguridad destinadas a las instalaciones nucleares y dirige reuniones internacionales periódicas en las que los profesionales pueden intercambiar conocimientos especializados y en las que tanto sus colegas como los expertos del OIEA pueden proporcionarles respuestas para resolver los problemas más acuciantes.

El OIEA también incorpora evaluaciones de la seguridad de la información en su Servicio internacional de asesoramiento sobre protección física (IPPAS).

El IPPAS –un servicio de examen integral disponible para todos los países que cuentan con materiales e instalaciones nucleares– presta asesoramiento a los Estados sobre los medios más eficaces de proteger sus materiales nucleares y radiológicos.

Hay muchas organizaciones que trabajan para afrontar las crecientes ciberamenazas. Es importante crear asociaciones para actuar en estas esferas. El OIEA ha colaborado con la Organización Internacional de Policía Criminal - INTERPOL y con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) en la realización de ejercicios internacionales, así como en la elaboración de documentos de orientación sobre ciberseguridad y en actividades de capacitación.

El ejercicio internacional @TOMIC 2012, sobre ciberseguridad y sucesos relacionados con la seguridad física nuclear, incluido el análisis forense nuclear, es un ejemplo de la participación del OIEA en actividades internacionales encaminadas a reforzar el conocimiento de la ciberseguridad para proteger los activos nucleares y otros materiales radiactivos. Este ejercicio, patrocinado por los Países Bajos, contó con 150 participantes de 40 países. El próximo ejercicio –@TOMIC 2014– se celebrará en 2014.

"Por el respeto de que goza en el mundo nuclear, el OIEA puede desempeñar una función estimulante y rectora tanto en la elaboración de directrices o protocolos como en el fomento del conocimiento de las medidas de ciberseguridad," dice el Sr. Govers, organizador de los ejercicios @TOMIC.

Las amenazas de siempre

Según el Sr. Dudenhoeffer, es importante que los Estados Miembros perciban las semejanzas entre las amenazas actuales y las que afrontaban hace 50 años.

"La amenaza sigue siendo la misma. Siempre han existido elementos criminales que tratan de robarles o de chantajearles. Siempre han existido individuos que se oponen a ustedes y a su labor, ya se trate de terroristas o de empleados descontentos. Siempre ha habido que proteger a las instalaciones nucleares y radiológicas contra estas amenazas. La gran diferencia es que ahora esos individuos pueden utilizar sistemas informáticos in situ o actuar a distancia para llevar a cabo su trabajo sucio," dice este experto en seguridad física nuclear.

Sasha Henriques, División de Información Pública del OIEA.

El OIEA ha implantado varios programas destinados a educar a los Estados acerca de estas cuestiones, ayudarlos a gestionar el problema y defenderse.

Las ciberamenazas representan un desafío mundial. El OIEA presta apoyo a los Estados en sus esfuerzos por elaborar y poner a prueba medidas de seguridad informática para proteger las instalaciones nucleares.

(Fotografía: istockphoto.com)