Hacer frente a las amenazas en materia de seguridad informática

La evolución del programa de asistencia del OIEA

Vasiliki Tafili

El cambio a sociedades de redes digitales, en las que las actividades cotidianas están interrelacionadas con la ayuda de sistemas computarizados, inteligencia artificial (IA) y tecnologías digitales, ha repercutido considerablemente en la seguridad nuclear tecnológica y física. No se puede insistir lo suficiente en el papel esencial que desempeñan las tecnologías digitales en el mantenimiento de las funciones de seguridad tecnológica y de seguridad física en las instalaciones dedicadas a la manipulación de material nuclear u otros materiales radiactivos.

"Los sistemas computarizados y las tecnologías digitales son vitales para las instalaciones y las actividades conexas en las que se utilizan materiales nucleares y otros materiales radiactivos", señala Elena Buglova, Directora de la División de Seguridad Física Nuclear del OIEA, que hace hincapié en la necesidad de que todos los países apliquen programas de seguridad informática y mejoren la defensa en profundidad de la seguridad nuclear. "A medida que avanza la tecnología, proteger la confidencialidad, la integridad y la disponibilidad de información y activos de carácter estratégico exige una vigilancia constante para prevenir y mitigar los riesgos, así como un sólido programa de seguridad informática y seguridad física de la información".

La necesidad de hacer frente a las amenazas a la seguridad informática, los ciberataques malintencionados y cualquier vulnerabilidad potencial que puedan introducir las tecnologías digitales, así como la importancia de la seguridad informática para la seguridad nuclear, se determinaron por primera vez en una resolución sobre seguridad física nuclear adoptada por la Conferencia General del OIEA en su quincuagésima quinta reunión ordinaria, en 2011. En ella se tomó conocimiento de los esfuerzos del OIEA "para fomentar la sensibilización a la creciente amenaza de los ataques cibernéticos y sus posibles consecuencias para la seguridad física nuclear". Esta resolución también alentó al OIEA a elaborar documentos de orientación apropiados, celebrar cursos de capacitación y acoger más reuniones de expertos dedicadas específicamente a la ciberseguridad en las instalaciones nucleares a fin de ayudar a los países a protegerse de los ataques cibernéticos.

"En seguimiento de la resolución de la Conferencia General de 2011, las actividades del OIEA se centraron en mejorar las capacidades de seguridad informática a nivel de los Estados y de las instalaciones", expresa la Sra. Buglova, que añade que estas actividades se incluyeron en los Planes de Seguridad Física Nuclear posteriores del OIEA, incluidos los detalles de la realización actual de las actividades de seguridad informática del OIEA que se describen a grandes rasgos en el Plan de Seguridad Física Nuclear para 2022-2025.

¿Cómo ayuda el OIEA a los países a desarrollar o mejorar su seguridad informática?

El establecimiento de un programa de seguridad informática sólido y actualizado es un elemento clave para proteger a los países de los ciberataques en todo tipo de infraestructuras críticas. El OIEA ha sido ágil a la hora de prestar asistencia a los países en todas las fases de desarrollo de los programas nacionales de seguridad informática y seguridad física de la información, asistencia que ha comprendido la facilitación de documentos de orientación y actividades de capacitación.

Cuatro publicaciones de orientaciones de la *Colección de Seguridad Física Nuclear del OIEA* y otras tres publicaciones técnicas ofrecen asesoramiento sobre seguridad informática y seguridad física de la información. Esas orientaciones pueden servir de base para la elaboración de marcos nacionales de seguridad informática, incluidas las estrategias nacionales, así como para los reglamentos y la capacitación en materia de seguridad informática.

Un principio clave de la orientación del OIEA es preservar las funciones críticas en las instalaciones nucleares protegiendo la información y los sistemas computarizados para mantener un entorno seguro desde el punto de vista tecnológico y físico respecto de las instalaciones y los materiales. Esto se logra desarrollando un programa de seguridad informática (véase la página 6), identificando las funciones de seguridad física nuclear, utilizando la gestión del riesgo para determinar las consecuencias potenciales de una seguridad comprometida, definiendo el nivel de seguridad informática necesario para los activos digitales de carácter estratégico y aplicando un enfoque graduado y los conceptos de defensa en profundidad en materia de seguridad informática. Estos elementos deberían diseñarse e implantarse de forma que eviten la puesta en riesgo y ayuden a aumentar la capacidad del explotador para detectar y responder a las intrusiones, así como para mitigar el impacto potencial de los ciberataques.

A solicitud de los países, el OIEA ofrece diversas oportunidades de capacitación a distintos públicos destinatarios, entre los que se encuentran las autoridades competentes, los explotadores, los proveedores y otras entidades que tengan responsabilidades en la puesta en práctica de la seguridad informática. Estos también podrían beneficiarse de los conocimientos especializados del OIEA en la realización de ejercicios de seguridad informática como parte del programa de seguridad física nuclear.

Además, hay cuatro cursos de aprendizaje electrónico sobre seguridad informática gratuitos que están disponibles en árabe, chino, español, francés, inglés y ruso en la Ciberplataforma de

Aprendizaje para la Enseñanza y la Capacitación en Red del OIEA, y se puede acceder a ellos inscribiéndose o a través de una cuenta NUCLEUS. En breve también estará disponible una plataforma de capacitación virtual nueva e innovadora (véase la página 12).

Paralelamente, el OIEA presta apoyo a ejercicios nacionales o regionales de seguridad informática como parte de su labor para concienciar sobre la amenaza de los ciberataques y sus posibles efectos en la seguridad física nuclear. Los ejercicios presentan diferentes escenarios en los que un ataque contra la protección física y los sistemas electrónicos tiene por objetivo directo o indirecto sistemas computarizados y la información de carácter estratégico.

Las actividades de investigación complementan las actividades de seguridad informática del OIEA, principalmente a través del mecanismo consolidado de proyectos coordinados de investigación. En los últimos años se han puesto en marcha proyectos de esta índole para fomentar la labor de la comunidad mundial de investigadores en materia de seguridad informática y seguridad física de la información e incrementar el nivel de preparación para hacer frente a los nuevos desafíos y riesgos (véase la página 18).

¿Qué nos depara el futuro?

El programa de seguridad informática del OIEA para la seguridad física nuclear está en constante evolución. El hecho de que los reactores modulares pequeños y los reactores avanzados dependan de tecnologías avanzadas y sistemas de instrumentación digital, las repercusiones previstas de la IA y la aparición de entornos de aprendizaje virtuales presentan desafíos y ámbitos respecto de los que cabe ampliar el apoyo a los Estados.

“Estamos presenciando una concienciación cada vez mayor de las implicaciones potenciales o reales para la seguridad nuclear tecnológica y física entre países, órganos reguladores, explotadores y otras partes interesadas”, afirma la Sra. Buglova. “Debido al importante crecimiento previsto en el uso de aplicaciones nucleares con fines pacíficos, en concreto los programas nucleoeléctricos, es indispensable considerar la seguridad informática y física de la información como una parte integrante de la seguridad física nuclear”.

Ciberataque

El término “ciberataque” se utiliza para describir un acto doloso con la intención de robar, alterar o destruir un objetivo específico, o impedir el acceso a este, mediante el acceso no autorizado a un sistema computarizado susceptible (o mediante acciones dentro de él). Los ciberataques ponen en peligro la confidencialidad, la integridad o la disponibilidad (o una combinación de estas propiedades) de la información de carácter estratégico dentro de un recurso digital de carácter estratégico, o de ese recurso, y pueden utilizarse para llevar a cabo o facilitar un acto doloso contra una instalación o una actividad u otro acto delictivo o intencional no autorizado que guarde relación con materiales nucleares u otros materiales radiactivos.

Un ciberataque puede llevarse a cabo a través del acceso físico directo a la información o a los recursos de información o a través del acceso electrónico, o mediante una combinación de ambos, y puede ser llevado a cabo directamente por un adversario o por un agente interno (o con su ayuda) influenciado deliberadamente o no por un adversario.

Los ciberataques, una vez detectados, deberían tratarse como incidentes de seguridad informática.

Esta definición está tomada de la publicación *Computer Security for Nuclear Security (Colección de Seguridad Física Nuclear del OIEA* Nº 42-G)