Cómo los ejercicios de seguridad informática ayudan a aumentar la preparación para responder a los ciberataques en la esfera de la seguridad física nuclear

Emma Midgley

Históricamente, las instalaciones nucleares se han concentrado en asegurar su material nuclear frente a ataques dolosos a través de medidas de protección física como armas de fuego, guardias y verjas. Estas medidas resultan efectivas aún hoy para amurallar las instalaciones nucleares, impidiendo el robo de material nuclear u otros materiales radiactivos, el sabotaje o el acceso no autorizado a los sistemas de control. Sin embargo, en las últimas décadas, la amenaza de los ciberataques se ha intensificado, en un mundo que tiende cada vez más a la digitalización. Cualquier país, incluso los que cuentan con los programas de investigación y energía nucleoeléctrica más avanzados, puede ser vulnerable a un ataque. Se ha hecho necesario elaborar marcos nacionales de seguridad informática y de respuesta contra las ciberamenazas a las instalaciones nucleares. Mediante ejercicios a gran escala, el OIEA brinda asistencia a los países para mejorar su protección contra los ciberataques y los ayuda a mejorar sus estrategias de detección y respuesta a los ciberataques contra las instalaciones nucleares.

El OIEA ha desarrollado ejercicios de seguridad informática para centrales nucleares e instalaciones radiológicas que se han llevado a cabo a escala nacional en todo el mundo. Estos ejercicios permiten a los países practicar y preparar su respuesta ante el peor de los escenarios posibles de vulneración de la ciberseguridad en una instalación nuclear. Los escenarios teóricos permiten determinar los puntos débiles de las políticas, los procedimientos y los procesos, e identificar las lagunas que deben colmarse mediante técnicas de mitigación, creación de capacidades y/o cambios organizativos. Además de ayudar a los Estados en la realización de ejercicios a gran escala para poner a prueba la seguridad informática en las instalaciones nucleares, las orientaciones del OIEA sobre seguridad física nuclear centradas en la seguridad informática también constituyen un recurso esencial que puede permitir a los países poner en marcha importantes medidas de seguridad informática para detectar, prevenir y responder a los ciberataques.

“Es fundamental desarrollar políticas, funciones y responsabilidades definidas y procedimientos detallados de respuesta a los incidentes de seguridad informática antes de que se produzca un incidente —afirma Trent Nelson, Oficial Superior de Seguridad Informática y de la Información de la División de Seguridad Física Nuclear del OIEA—. Esta es la esfera en la que el OIEA puede ayudar en muchos aspectos que van desde ejercicios y orientación, hasta compartir prácticas y procedimientos óptimos para garantizar una comunicación eficaz y una sólida protección de la seguridad”.

La vulnerabilidad de las instalaciones nucleares frente a los ciberataques se debe a varios factores, como las personas, la complejidad de la cadena de suministro y la información delicada compartida entre las múltiples partes interesadas que utilizan los sistemas informáticos que sustentan las funciones nucleares.

“Pensemos en un ataque en el que se compromete a un proveedor y se falsifica una orden de trabajo, haciendo que un técnico de confianza con acceso autorizado lleve a cabo una acción que sea ligeramente incorrecta —dice Trent Nelson—. Esta es una de las muchas formas que agentes con fines dolosos podrían encontrar para burlar los sistemas de seguridad”.

Un elemento importante para reducir el impacto que un ciberataque podría tener es la sensibilización y la comunicación efectiva entre las partes interesadas, ya que cualquiera de estos grupos, o de los individuos que forman parte de ellos, puede ser objeto de un ataque por parte de agentes dolosos. En la defensa de las instalaciones nucleares hay cuatro actores claves: el órgano regulador; el explotador de la instalación; las organizaciones de apoyo técnico (equipos de respuesta a incidentes de seguridad informática (CSIRT) y/o centros de operaciones para la seguridad informática); y las organizaciones externas, como proveedores y organizaciones de apoyo. La realización de ejercicios es una buena manera de poner a prueba las comunicaciones, la presentación de informes y las notificaciones entre las partes interesadas, así como de verificar y validar la seguridad tecnológica y la seguridad física de las estructuras organizativas.

Un elemento importante para reducir el impacto que un ciberataque podría tener es la sensibilización y la comunicación efectiva entre las partes interesadas.
(Imagen: AdobeStock)

Aunque en un escenario ideal a los ciberatacantes les resultaría imposible penetrar en los sistemas de seguridad informática de las instalaciones nucleares, la naturaleza cambiante de los agentes con fines dolosos, y la falibilidad de la naturaleza humana, hacen que sea casi imposible predecir cómo se desarrollará el próximo ataque a gran escala. Por lo tanto, la detección oportuna de los ataques es clave. En un ejercicio realizado recientemente en Eslovenia, un ciberataque teórico ayudó a verificar y validar las capacidades de detección y respuesta para defenderse de los ciberataques.

"La seguridad informática no es un proyecto ni un proceso, sino un viaje de por vida que requiere un esfuerzo, una atención y una práctica continuos —declara Samo Tomažič, Jefe de la División de Ciberseguridad de la Administración Eslovena de Seguridad Nuclear—. Ejercicios como el realizado en Eslovenia permiten a todas las entidades pertinentes del sector nuclear evaluar la solidez de sus planes de respuesta a incidentes en caso de ser objeto de un ciberataque".

En caso de incidente grave de seguridad informática que pudiera contribuir a un suceso de seguridad nuclear tecnológica o física, se debería contar con la ayuda de un CSIRT, además de con las partes interesadas habituales de una instalación nuclear. Un incidente de este tipo podría ocasionar, por ejemplo, el quebrantamiento de políticas o procedimientos de seguridad; efectos sobre los activos o sistemas digitales sensibles; o la pérdida de información sensible, así como del control de funciones críticas para la seguridad nuclear.

En este caso, una vez que se identifica un incidente de seguridad informática o se detecta que esta ha sido comprometida, el CSIRT trabaja con las partes interesadas de la instalación para investigar el incidente, recopilar datos forenses, analizar qué ocurrió y dónde, y prestar asistencia para contener y erradicar la intrusión a fin de ayudar a los explotadores a volver a poner en línea la instalación nuclear. Al final de la respuesta, se reúnen pruebas de informática forense para ayudar en cualquier investigación penal sobre el ataque y garantizar un intercambio de información eficaz con miras a seguir reforzando las medidas de seguridad informática en la instalación nuclear en el futuro.

En el ejercicio de Eslovenia, la detección de ciberataques fue esencial para poder responder a este incidente de seguridad teórico y probar y validar los procedimientos de respuesta a incidentes. Estos ejercicios sirven para poner a prueba la relación entre seguridad tecnológica, seguridad física y preparación para emergencias, y refuerzan los regímenes de seguridad física nuclear mediante la determinación de posibles puntos débiles y el desarrollo de los cambios necesarios para mejorar su preparación global ante posibles amenazas a la ciberseguridad. Además, estos ejercicios brindan la oportunidad de poner a prueba los canales de comunicación nacionales e internacionales para las notificaciones y la presentación de informes. En general, la realización periódica de ejercicios de seguridad informática es un aspecto importante del mantenimiento de la seguridad física de las instalaciones nucleares.