Contrarrestar las amenazas en un mundo cada vez más digitalizado

Wolfgang Picot

En mayo de 2022, el Instituto Austríaco de Tecnología (AIT) pasó a ser el primer centro colaborador del OIEA en seguridad informática y seguridad física de la información en aras de la seguridad física nuclear. El AIT presta apoyo a cursos y ejercicios internacionales y regionales de capacitación en el ámbito de la seguridad informática para instalaciones y actividades nucleares, desarrolla módulos de demostración técnica para crear más conciencia acerca de las ciberamenazas, y contribuye a la elaboración de materiales de capacitación para el nuevo Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear, ubicado en Seibersdorf.

Hablamos con el Director del Centro de Seguridad Tecnológica y Física del AIT, Helmut Leopold, para comprender mejor en qué consiste esta cooperación.

P: ¿Cuáles son, en general, los riesgos y amenazas emergentes en materia de seguridad informática?

R: Hoy en día muchos dispositivos digitales modernos se construyen pensando en redes más extensas.

Muchos de ellos necesitan acceso a Internet para funcionar. Todo desarrollo de software entraña posibles errores que pueden dar lugar a vulnerabilidades. El número de amenazas contra la seguridad física que afectan al funcionamiento de los sistemas de tecnologías de la información (TI) aumenta a la luz de la escasa protección de las interfaces y la irresponsabilidad de los usuarios. Los atacantes se aprovechan de las vulnerabilidades de los sistemas digitales para lograr el acceso.

El desarrollo de métodos y herramientas de ataque discurre en paralelo al de los procesos de innovación digital. En Internet se encuentran fácilmente programas informáticos para piratas informáticos, lo que facilita los ataques, incluso para atacantes menos competentes. Nos enfrentamos a un diverso ecosistema de ciberataques impulsado por la delincuencia organizada, el espionaje económico e industrial y el terrorismo cibernético.

Así pues, hoy en día, usuarios, empresas y autoridades se ven amenazados por un amplio espectro de ciberataques que, acompañados de campañas específicas de desinformación, pueden afectar la infraestructura digital de Estados enteros, sacudiendo así los cimientos de nuestras sociedades.

P: ¿La industria nuclear se enfrenta a los mismos desafíos?

R: Los negocios y los distintos consumidores utilizan principalmente tecnologías de la información (TI) basadas en datos y orientadas a la comunicación. Por el contrario, las instalaciones de producción y las infraestructuras críticas emplean la llamada tecnología operativa (TO) que monitoriza y controla los comportamientos y los resultados prácticos de procesos de producción definidos. Tradicionalmente, la TO ha estado mucho menos interconectada que la TI, pero los avances tecnológicos han acercado a estos dos campos, haciendo que el *software* y los dispositivos de TO se conecten, cada vez más, a redes de mayor amplitud.

Este desarrollo resulta problemático, pues hay menor conciencia acerca de la ciberseguridad en el campo de la TO que en el de la TI.

Por ello, estas nuevas amenazas para la seguridad física de las TI se vuelven pertinentes para la TO de producción industrial e infraestructura crítica. Asimismo, esta cuestión es cada vez más importante para la industria nuclear, que tradicionalmente tenía un enfoque conservador y mantenía aislados los sistemas de control.

P: ¿Qué actividades lleva adelante el AIT con el fin de mejorar la ciberseguridad en el ámbito de la seguridad física nuclear?

R: El programa de investigación del AIT examina cómo escenarios de amenazas cambiantes podrían repercutir en los sistemas de TO, y tiene por objeto desarrollar conocimientos técnicos y nuevas soluciones para aumentar la resiliencia de las infraestructuras críticas frente a los ciberataques. Este trabajo constituye la base para el desarrollo de nuevas normas mundiales de seguridad física, procedimientos de certificación para elementos críticos del sistema y nuevas arquitecturas del sistema que incorporen medidas sólidas de ciberseguridad en los sistemas de TO desde la etapa inicial del diseño.

El AIT ofrece asimismo una enseñanza y capacitación integrales como preparación frente a ataques contra la ciberseguridad. En simulaciones complejas de sistemas informáticos “virtualizados”, denominadas “cyber ranges”, los usuarios, los desarrolladores de sistemas, el personal de operación y los representantes gubernamentales reaccionan ante escenarios realistas de ciberataques. Esta clase de simulación es fundamental para garantizar que los sistemas de TI y TO son resilientes y pueden repeler eficazmente las ciberamenazas.

P: ¿Qué ventajas plantea el entorno de aprendizaje virtual desarrollado por el AIT y el OIEA?

R: La experiencia práctica es el proceso de aprendizaje más eficaz. El AIT y el OIEA desarrollaron un "cyber range" que ofrece la posibilidad de crear "gemelos digitales" de las infraestructuras digitales críticas existentes, en el que, además, se imparte capacitación en escenarios de aplicación muy realistas.

En él, los usuarios gubernamentales y de la industria pueden evaluar y someter a prueba la eficacia de los mecanismos de protección y los procesos institucionales u operacionales.

Las experiencias del "cyber range" respaldan la creación de capacidades de defensa sostenibles, tanto para las organizaciones públicas como privadas.

P: Además de la capacitación virtual, ¿de qué manera promueve el AIT la seguridad física nuclear con su trabajo y sus conocimientos especializados?

R: Podemos ayudar en la defensa frente a atacantes, por ejemplo, desarrollando software para monitorizar dispositivos perimetrales que suelen conectar las redes internas de las organizaciones a Internet. Antes de causar daños, los atacantes suelen servirse de estos dispositivos como puntos de entrada al sistema.

Aplicamos nuestra experiencia en detección de anomalías para entrenar el software de análisis que monitoriza los dispositivos perimetrales de uso común en un determinado tipo de instalación nuclear.

Ese software puede activar una alarma o adoptar contramedidas si un dispositivo actúa de forma extraña. Así, los operadores pueden detectar y desalentar prontamente los ciberataques antes de que estos puedan causar perjuicios significativos.

P: Hace un año, el AIT fue designado primer centro colaborador del OIEA en seguridad informática al servicio de la seguridad física nuclear, y sigue siendo el único centro de este tipo a día de hoy. ¿Qué significa esto para la labor del AIT?

R: Estamos sumamente orgullosos de haber sido designados centro colaborador, y seguimos brindando apoyo para impartir un curso regional de capacitación sobre seguridad informática aplicada a los sistemas de instrumentación y control en el sector nuclear. El curso se dictó dos veces en 2022, y algunos de los resultados prácticos de nuestro proyecto conjunto se emplearon para desarrollar una plataforma de aprendizaje virtual.

Asimismo, hemos participado en actividades relacionadas con la seguridad informática en el desarrollo de reactores modulares pequeños.

En la actualidad prestamos asistencia al OIEA para la preparación de la Conferencia Internacional sobre Seguridad Informática en el Mundo Nuclear: la Seguridad Física en aras de la Seguridad, que tendrá lugar en 2023 y en la que ofreceremos demostraciones de nuestra plataforma de capacitación virtual, presidiremos mesas redondas y presentaremos artículos relacionados con nuestra investigación en el sector, entre otras cosas.

P: ¿Cómo colabora el AIT con el Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear?

R: Hemos estado trabajando codo a codo con nuestros colegas del OIEA para desarrollar módulos de capacitación, demostraciones y ejercicios para el Centro de Capacitación y Demostración en materia de Seguridad Física Nuclear. Incorporamos módulos sobre seguridad informática en los cursos de capacitación relacionados con la protección física de materiales nucleares y otros materiales radiactivos, así como aquellos vinculados a la detección y respuesta en relación con materiales nucleares y otros materiales radiactivos no sometidos a control reglamentario. Este arreglo tiene por objeto reforzar el concepto de que la seguridad informática es un elemento integral e indisociable de la seguridad física nuclear.