Desarrollo de capacidades formativas. Simulación de escenarios en técnicas de investigación en ciberseguridad

Abstract: ante la evolución de las nuevas tecnologías relacionadas con la información y la comunicación y ante el uso generalizado de internet, es fundamental educar a la sociedad y a los profesionales de la ciberseguridad de los posibles riesgos asociados a un uso incorrecto de la tecnología.

Contenido:

1. CAPACITACIÓN EN CIBERSEGURIDAD

Con la capacitación y la labor formativa se persigue enseñar al usuario de la tecnología a detectar indicadores e identificar evidencias que sugieran una amenaza potencial contra los sistemas tecnológicos. También deben saber cómo analizar estos indicios, y anticipar o articular medidas de protección, contención o mitigación. Es decir, se ha de capacitar a los usuarios en la detección de indicadores de ciberamenaza sobre sistemas tecnológicos.

En este sentido, la cibervigilancia es el conjunto de procedimientos organizados dedicados a observar contenidos digitales que son transmitidos por diferentes canales de información, con el fin de detectar en ellos indicadores de ciberamenaza sobre sistemas tecnológicos.

La cibervigilancia tiene principalmente una función de ciberseguridad preventiva puesto que, por medio del análisis de contenidos circulando a través de internet, se marca el objetivo de cribar indicios que sugieran una amenaza potencial contra sistemas tecnológicos, analizar esos indicadores y anticipar o articular medidas de protección, contención o mitigación.

En algunas ocasiones, esos indicadores de ciberamenaza pueden incluir menciones directas o indirectas que sugieran intenciones de ciberataque contra sistemas tecnológicos; otras pueden ser proclamas incitando a atacar sistemas tecnológicos; otras, reivindicaciones comunicando que ya se ha llevado a cabo un ciberataque comprometiendo alguna infraestructura o dispositivo tecnológico conectado a internet; otras veces son exfiltraciones de información sensible previamente obtenida por procedimientos ilícitos o por un ciberataque a un sistema tecnológico.

En cualquiera de los casos, permanecer a la escucha de esos contenidos que se transmiten por internet es una tarea ineludible para la prevención y gestión de riesgos en el ciberespacio.

Por tanto, la formación continua en ciberseguridad es necesaria para poder prevenir, y tratar de manera oportuna, posibles incidentes de ciberseguridad. Por este motivo, el Centro Criptológico Nacional (CCN) desarrolla gran variedad de actividades formativas para lograr una mayor concienciación en este ámbito.

2. FORMACIÓN MEDIANTE LA SIMULACIÓN DE ESCENARIOS EN TÉCNICAS DE INVESTIGACIÓN

Los CSIRT[1] de referencia tienen la obligación de desplegar sus capacidades concentrando recursos tecnológicos y humanos especializados en la detección y seguimiento de contenidos maliciosos circulando por internet que puedan sugerir indicadores de ciberamenaza en el ámbito de su competencia.

La cibervigilancia, en tanto procedimiento organizado y sistematizado, se desarrolla a través de un conjunto de técnicas de observación que requieren del entrenamiento de recursos humanos especializados, profesionales dedicados a la prevención de amenazas en ciberseguridad.

En este sentido, dentro de su programa general de capacitación STIC (Seguridad de las Tecnologías de la Información y la Comunicación), el CCN-CERT imparte un Curso STIC de Cibervigilancia, en colaboración con el Instituto Nacional de Administración Pública, dirigido a funcionarios de la Administración Pública en España cuyo contenido está dedicado a proporcionar conocimientos básicos en la detección temprana y análisis de indicadores que pudieran constituir una ciberamenaza para las tecnologías.

Para complementar dicha formación, el CCN está desarrollando ELENA, una herramienta de entrenamiento en simulación de escenarios, que permitirá a los profesionales practicar técnicas de investigación en ciberseguridad. Todo ello, en un entorno de laboratorio asilado y simulado, programado con casos de uso ficticios. Así, ELENA se constituye como un complemento de entrenamiento práctico para los cursos STIC que el CCN ya desarrolla en el contexto de su plataforma ÁNGELES.

Con ELENA los alumnos tienen la oportunidad de practicar la resolución de casos de uso en ciberseguridad mediante la emulación de escenarios de investigación prototípicos, que un usuario dedicado a la ciberseguridad y a la cibervigilancia podría encontrarse en un entorno real. No obstante, al haber sido desarrollado como un simulador de escenarios, ELENA no conecta con ningún servicio o servidor en internet más allá de los repositorios propios del propio simulador, donde se almacenarán los contenidos necesarios para realizar la simulación de escenarios con los que ELENA sea programada.

Los escenarios simulados de ELENA para el entrenamiento serán ficticios y constarán de contenidos en distintos formatos (texto, audio y vídeo), lo que aportará a los usuarios una apariencia suficiente de realidad donde simular procedimientos de cibervigilancia.

[1] Computer Security Incident Response Team

Ante un entorno global de ciberamenazas, sofisticadas en sus capacidades, persistentes en sus intenciones ilícitas e innovadoras en sus tácticas de vulneración de sistemas tecnológicos; con los cursos STIC de cibervigilancia y con ELENA, el CCN cumple su función y compromiso de desarrollar actividades formativas destinadas a compartir con profesionales de la ciberseguridad las técnicas y procedimientos que permitan salvaguardar la integridad y continuidad de los servicios en el ciberespacio español en general y en las tecnologías de las Administraciones Públicas en particular.

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.02.06 23:14:46 +01'00'