Equipo Red Team, de Entelgy Innotec: cómo poner a prueba las capacidades de defensa

En los últimos años, ha quedado demostrado que las tradicionales medidas enfocadas a proteger los sistemas y equipos, el desarrollo de planes y políticas de seguridad o las auditorías que intentan analizar los riesgos de una organización frente a un ciberataque son insuficientes. Los atacantes suelen ser muy creativos y disruptivos y los sistemas de defensa de las organizaciones tardan demasiado en mejorar sus métodos de detección. De ahí la necesidad de contar con un equipo de Red Team que, como el de Innotec Security, división de Entelgy, ponga a prueba las capacidades de defensa de una organización.

La superficie de exposición cada vez es mayor y diariamente aparecen nuevos vectores de ataque, nuevas vulnerabilidades, nuevos dispositivos, nuevas aplicaciones, nuevas tecnologías y herramientas, por lo que las medidas adoptadas en cada caso deben ser evaluadas continuamente, adaptándose a estas nuevas circunstancias.

Los ciberdelincuentes tienen la característica de ser creativos y disruptivos y los sistemas de defensa de las organizaciones tardan demasiado en mejorar sus métodos de detección de ataques. Estas diferencias generan brechas de seguridad que son aprovechadas por los atacantes.

En este sentido, **Innotec Security**, división de Entelgy, como empresa referente del sector, ha desarrollado un servicio enfocado en la parte ofensiva de la ciberseguridad y de gran valor para sus clientes: el **Red Team**.

En concreto, propone una nueva metodología para conocer el nivel de exposición y riesgo de una organización, así como su capacidad de detección y respuesta. Para ello, se simula, en cierto modo, un combate militar entre dos equipos, el rojo (Red Team), formado por los profesionales de Innotec, y el azul (Blue Team), que vendría a ser la organización que se está analizando en su conjunto.

Este servicio de Red Team, uno de los principales de la compañía, está formado por un equipo independiente y multidisciplinar de profesionales técnicos, quienes están especializados en distintos dominios de la seguridad informática. Este equipo es el encargado, utilizando sus conocimientos técnicos avanzados, de simular ataques de todo tipo a una entidad, del mismo modo que los ejecutados por ciberdelincuentes.

Las variedades de escenarios reales creadas por estos profesionales se asocian a los principales riesgos del sector de la compañía que se analice, buscando siempre la simulación real, pero controlada, de estos ejercicios. Actualmente ya son varios los sectores que están requiriendo este tipo de ejercicios como practica principal para la identificación y gestión de riesgos tecnológicos.

Desde Innotec se ha desarrollado una metodología en la que confluye toda la experiencia de nuestro equipo en multitud de proyectos de carácter ofensivo.

La metodología está basada en la máxima de los ejercicios de Red Team, es decir, en la simulación de ataques técnicos incrementando progresivamente la complejidad, poniéndose en la piel de atacantes reales, buscando persistencia en los sistemas de la compañía y realizando movimientos laterales para exfiltrar información valiosa e identificar objetivos importantes de la compañía.

Nos basamos en **MITRE ATT&CK** (*Adversarial Tactics, Techniques, and Common Knowledge*), un conjunto de tácticas, técnicas y procedimientos basados en observaciones reales, creando escenarios específicos para cada cliente y sector.

Para llevar a cabo esta metodología y llegar a identificar el nivel de exposición y de riesgo que tiene la organización, es primordial ponerse en la piel del atacante, combinando los mismos métodos que utilizaría este, tanto a nivel de seguridad digital, seguridad física (intrusión en un edificio), seguridad humana o ciberinteligencia. El propósito no es otro que simular, de la forma más precisa posible, cómo actuaría el delincuente en una situación real.

El primer paso será **definir y planificar el ataque** que llevará acabo el Red Team hacia la organización, un ataque que, por cierto, siempre será dirigido. Esta fase llevará alrededor de dos semanas, durante la cuales se buscará información sobre la organización que permita dirigir el ataque.

Posteriormente, el **Reconocimiento externo** para ver qué activos pueden ser vulnerables con mayor probabilidad, con el objetivo de buscar un compromiso inicial. Por ejemplo, se lleva a cabo un acceso no autorizado a los sistemas a través de cualquier pequeño resquicio en el ámbito digital, como pueden ser el perímetro, Wi-Fi o correo electrónico.

Uno de estos activos podría ser la penetración física a la organización, si se ha con-

Figura 1: Metodología del servicio

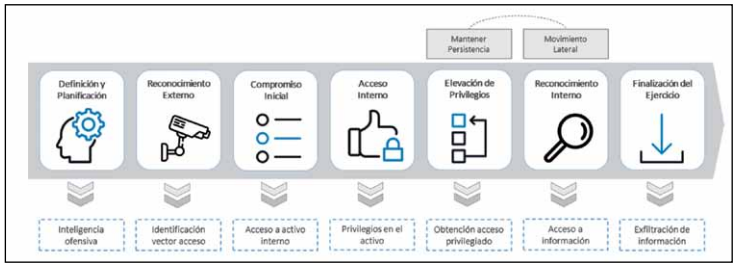

Figura 2: Proceso metodológico del equipo Red Team de Innotec Security

siderado que este es el más vulnerable. El uso de técnicas de ingeniería social es clave para realizar esta intrusión. Una llamada de teléfono fingiendo ser alguien de confianza, un correo electrónico suplantando la identidad de una persona, contacto a través de Facebook o el regalo de un USB infectado son solo algunos de los ejemplos de técnicas que se podrían utilizar para comprometer a la organización.

Una vez logrado un **primer compromiso** inicial de la compañía, el siguiente objetivo será lograr **acceso interno** y que el Red Team pueda moverse por diferentes elementos de la organización y conseguir elevar privilegios, de tal forma que logre persistencia y sea capaz de regresar a la organización cada vez que le interese. De esta forma, el atacante obtendrá libertad para moverse por toda la organización y así alcanzar los objetivos que se haya marcado, como puede ser el acceso a nombres, horarios, claves, números de tarjeta, etc.

Realizado el ataque, el equipo de Red Team comienza a **dejarse ver** poco a poco para comprobar los mecanismos que tiene la organización para detectar y dar respuesta a un incidente. En otras palabras, el Red Team va dejando cada vez más ventaja al Blue Team para ver cuánto tarda este en descubrir que le ha estado atacando. Esto último es esencialmente el objetivo final de este servicio de Innotec: descubrir hasta qué punto está la defensa de una organización preparada frente a un ataque. De forma más concreta, lo que se busca es verificar de forma continua la efectividad de los planes de actuación, las medidas defensivas implementadas o el correcto funcionamiento de las políticas del propio equipo de seguridad interno de la organización.

Por último, la fase final de este servicio de Red Team de Innotec, y que supone uno de sus puntos diferenciadores, consiste en la **formación de la organización**, conocida como Blue Team Training, donde se evalúan las acciones tomadas durante la simulación y determina la evolución de las defensas que se puedan implementar a nivel organizacional, de procedimientos y de arquitectura para evitar futuras intrusiones similares.

Formar a la organización para evitar futuros ataques

Para conseguir que la seguridad de la organización sea cada vez más segura, el equipo de Red Team de Innotec lleva a cabo una serie de sesiones formativas con algunos miembros del Blue Team para aprender de lo sucedido durante el ataque. Se reúnen los hackers del Red Team con el Blue Team de la organización y se lleva a cabo el Blue Team Training, una de las acciones que realmente más valor aporta a la organización.

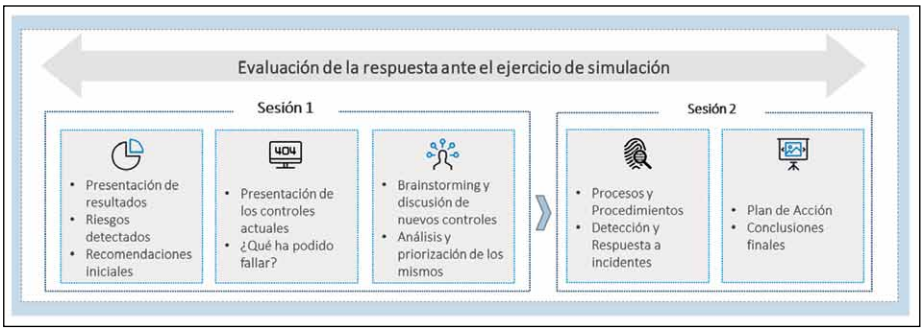

Figura 3: Evaluación de la respuesta ante el ejercicio de simulación

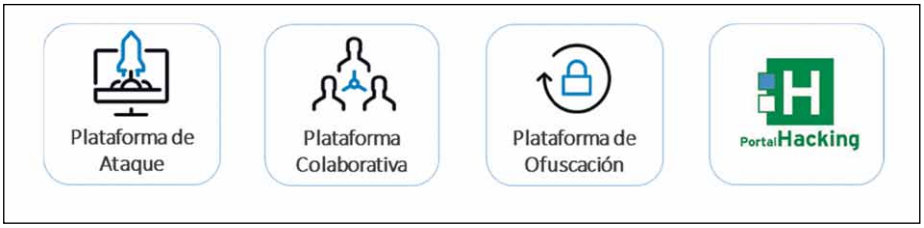

Figura 4. Plataformas que se utilizan en un ejercicio de Red Team

Esta formación no consiste en mostrar al Blue Team cómo configurar el *firewall*, por poner un ejemplo, sino que el objetivo es básicamente utilizar el conocimiento del equipo de Innotec dentro de la parte ofensiva para dar esa visión al equipo de defensa.

A modo de resumen, la metodología del Blue Team Training estaría formada por los siguientes puntos:

1. Resultados del ejercicio: presentación de riesgos, resultados y recomendaciones de buenas prácticas.

2. Formación ofensiva: exposición de técnicas, tácticas, procedimientos de ataques habituales.

3. Análisis y ataque: *workshop* para el análisis de la infraestructura y ataques que se pueden realizar sobre ella.

4. Simulaciones–*Wargame*: *workshop* con ejercicios teóricos de ataque–defensa.

5. Planes de actuación: *workshop* para la revisión y definición de planes de acción.

Como resultado final del servicio se obtienen propuestas de mejora sobre los procedimientos, procesos y controles de seguridad para incrementar la efectividad de las capacidades de prevención, detección, investigación y respuesta de la organización.

Aspectos diferenciales de Innotec

El equipo de Innotec hace uso de herramientas propias que permiten realizar el control, seguimiento de las tareas y actividades durante el desarrollo de la ejecución del servicio, el cual cuenta con ciertas características que lo diferencian de sus competidores: servicio interno de informes de amenazas con orientación al conocimiento de técnicas de ataque adaptado a la casuística de los clientes; formación específica para los gestores del servicio de Red Team por parte del cliente; conocimiento avanzado en tácticas, técnicas y procesos específicos de Red Team, modelando datos para medir resultados, gracias a la experiencia adquirida en multitud de proyectos; gestión de resultados y *remediaciones* de vulnerabilidades encontradas en el servicio; y colaboración con el Blue Team.

Además, el equipo encargado de la ejecución del servicio de Red Team cuenta con un alto número de profesionales con las certificaciones más avanzadas del sector, como son OSCE, CREST, OSCP, OSWP, etc.

Por último, cabe destacar que Innotec fue responsable, junto a **Bankia**, de la organización de las I Jornadas de Red Team en España, celebradas el pasado 25 de octubre en el Auditorio Torre Bankia de Madrid. Este encuentro, que acogió a más de 150 asistentes, contó con un alto grado de aceptación. ■

Enrique Domínguez
Strategy Director
Nacho García Egea
Strategy Manager
contacta@innotecsystem.com
ENTELGY INNOTEC SECURITY