GUILLERMO GONZALEZ Y EDUARDO ARRIOLS. INNOTEC SYSTEM

Red Team: Pensando como el enemigo

«Conócete a ti mismo y conoce a tu enemigo». Esta máxima extraída del ensayo «El Arte de la Guerra» del filósofo y militar chino, Sun Tzu (s. II a.C.), resume como pocas la estrategia a seguir en cualquier conflicto y es la que subyace en la creación de los denominados Red Team, equipos altamente cualificados que simulan intrusiones reales y controladas en una organización. Su desarrollo se debe a la necesidad de enfrentarse a un atacante, cada vez más sofisticado, que cuenta con un buen número de factores a su favor (recursos económicos, tiempo, conocimiento, herramientas y tecnología, legislación laxa, etc.), y que los empleará sin dudarlo para ocasionar el mayor daño posible a su objetivo, bien sea económico, de imagen o de reputación.

TENER una visión global de la situación exacta de la organización en todos los frentes (digital, físico y de las personas) y, sobre todo, conocer las técnicas intrusivas del atacante y su razonamiento, se vuelven indispensables para defender los activos críticos de cualquier organización.

El concepto de Red Team proviene del ámbito militar y es utilizado en contraposición con el de Blue Team; englobados ambos dentro de las actividades de War Gamming o simulaciones de guerra, donde un equipo adquiere el rol de atacante (Red) y otro de defensor (Blue). Este tipo de ejercicios han venido realizándose de forma continuada desde hace décadas por los ejércitos de un buen número de países, y suponen uno de los entrenamientos más eficaces para conocer su estado de la seguridad, sus flancos débiles y, sobre todo, sus capacidades defensivas y de reacción ante cualquier intrusión.

A raíz de los atentados del 11-S en el año 2001, esta práctica militar de ataque y defensa se fue trasladando e intensificando a la comunidad de inteligencia (tanto civil como militar) y al ámbito privado, particularmente al sector de la seguridad de las grandes compañías contratistas del gobierno estadounidense.

De las tácticas militares a las de seguridad

Hoy en día, los equipos Red Team, como el que posee la empresa de ciberseguridad InnoTec (del Grupo Entelgy), han adaptado estas tácticas militares a los entornos de seguridad, con el fin de dar un paso más en la defensa de los activos críticos de una organización.

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 verificar que las acciones llevadas a cabo son las correctas, son acertadas pero no suficientes. En realidad, permiten verificar la seguridad de ciertos activos, pero ni mucho menos la seguridad global de la organización.

No olvidemos que la superficie de exposición cada vez es mayor y que diariamente aparecen nuevos vectores de ataque, nuevas vulnerabilidades, nuevos dispositivos, nuevas aplicaciones, nuevas tecnologías y herramientas y que, las medidas adoptadas en cada caso deben ser evaluadas continuamente, adaptándose a estas nuevas circunstancias.

Esta situación queda patente al analizar los incidentes relacionados con ataques dirigidos y APTs, acrónimo de Advanced Persistent Threat (Amenaza Persistente Avanzada), en donde existe un alto nivel de sofisticación y recursos, y en donde se utilizan la mayoría de las veces una combinación de vectores de entrada tanto en el ámbito digital (malware, vulnerabilidades, exploits, etc.), como en el físico (controles de acceso, redes Wi-Fi, ATM, etc.) y sobre el personal de la organización (ingeniería social).

Ataques donde se busca el camino más corto para penetrar en la fortaleza en la que, desgraciadamente, en un alto porcentaje de casos, se consigue entrar. Ante ello es el equipo defensivo (Blue Team) el que tiene que estar preparado para detectarlo con rapidez y responder de la manera más eficaz antes de su propagación.

En la piel del atacante

Precisamente para preparar esta defensa, se hace necesario realizar simulaciones de intrusiones reales y controladas de ejercicios Red Team; es decir, ponerse en la piel del atacante, reproduciendo todos sus pasos antes de lle-