**Tipos de agentes de amenazas**

Para ser un profesional de seguridad efectivo, una habilidad importante que deberás desarrollar es poder anticiparte a los ataques. Para lograrlo, debes mantener una mentalidad abierta y flexible en cuanto a su procedencia. Antes, aprendiste sobre las **superficies de ataque**, que son todas las vulnerabilidades potenciales que un agente de amenaza podría explotar.

Las redes, los servidores, los dispositivos y el personal son ejemplos de superficies de ataque que pueden explotarse. Con frecuencia, los equipos de seguridad de todos los tamaños se encuentran defendiendo estas superficies debido al panorama digital en expansión. La clave para defender cualquiera de ellos es limitar su acceso.

En esta lectura, profundizarás en los agentes de amenaza y los tipos de riesgos que representan. También explorarás las características más comunes de una superficie de ataque que los agentes de amenaza pueden explotar.

**Agentes de amenaza**

Un **agente de amenaza** es cualquier persona o grupo que plantea un riesgo para la seguridad. Esta definición a grandes rasgos abarca a personas tanto dentro como fuera de una organización. También incluye a personas que intencionalmente representan una amenaza y quienes ponen en riesgo los activos por accidente. ¡Es una amplia variedad de personas!

Por lo general, los agentes de amenaza se dividen en cinco categorías según sus motivaciones:

* La **competencia** refiere a las empresas rivales que representan una amenaza porque podrían beneficiarse de la información filtrada.
* Los **actores estatales** son agencias de inteligencia del gobierno.
* Los **sindicatos criminales** son grupos organizados de personas que ganan dinero mediante actividades delictivas.
* Las **amenazas internas** pueden ser cualquier persona que tenga o haya tenido acceso autorizado a los recursos de una organización. Esto incluye a los empleados que comprometen los activos por accidente o individuos que los ponen en riesgo de manera intencional, para su propio beneficio.
* **Shadow IT** hace referencia a individuos que utilizan tecnologías que carecen de gobernanza de TI. Un ejemplo común es cuando un empleado usa su correo electrónico personal para enviar comunicaciones relacionadas con el trabajo.

En la superficie de ataque digital, estos agentes de amenaza a menudo obtienen acceso no autorizado al hackear los sistemas. Por definición, un **hacker** es cualquier persona o grupo que utiliza computadoras para acceder a datos sin autorización. Al igual que el término actor de amenazas, hacker es también un término general. Cuando se usa solo, el término no consigue captar las intenciones de un agente de amenaza.



**Tipos de hackers**

Debido a que la definición formal de hacker es amplia, el término puede ser un poco ambiguo. En seguridad, corresponde a tres tipos de personas en función de su intención:

1. Hackers no autorizados
2. Hackers autorizados o éticos
3. Hackers semiautorizados

Un hacker no autorizado, o hacker no ético, es un individuo que utiliza sus habilidades de programación para cometer delitos. A los hackers no autorizados también se los conoce como hackers maliciosos. El nivel de habilidad varía ampliamente dentro de esta categoría de hackers. Por ejemplo, existen hackers con habilidades limitadas que no pueden escribir su propio software malicioso, a veces llamado *script kiddies* (niñitos del script)**.** Este tipo de hackers no autorizados llevan a cabo ataques mediante un código preescrito que obtienen de otros hackers más hábiles.

Los hackers autorizados, o éticos, son personas que utilizan sus habilidades de programación para mejorar la seguridad general de una organización. Estos incluyen a miembros internos de un equipo de seguridad que se ocupan de probar y evaluar los sistemas para asegurar la superficie de ataque. También se trata de proveedores de seguridad externos y hackers independientes que algunas empresas incentivan para encontrar y reportar vulnerabilidades, una práctica llamada programas de **recompensas por errores**.

Por lo general, los hackers semiautorizados son individuos que podrían violar estándares éticos, pero que no son considerados como maliciosos. Por ejemplo, un **hacktivista** es una persona que podría usar sus habilidades para lograr un objetivo político. Podría explotar las vulnerabilidades de seguridad de una empresa de servicios públicos para concientizar sobre su existencia. Las intenciones de este tipo de agentes de amenaza suelen consistir en exponer los riesgos de seguridad que deben abordarse antes de que un hacker malicioso los encuentre.

**Amenazas persistentes avanzadas**

Muchos hackers maliciosos consiguen ingresar en un sistema, causan problemas y luego se marchan. Pero en algunas ocasiones, los agentes de amenaza se quedan. Este tipo de eventos se conocen como amenazas persistentes avanzadas, o APT.

Una **amenaza persistente avanzada (APT)** hace referencia a los casos en que un actor de amenazas mantiene el acceso no autorizado a un sistema durante un período prolongado de tiempo. El término se asocia principalmente con los estados nacionales y los agentes patrocinados por el Estado. Por lo general, una APT se ocupa de vigilar un objetivo para recopilar información. Luego esta información se utiliza para manipular los servicios gubernamentales, de defensa, financieros y de telecomunicaciones.

El hecho de que el término esté asociado con agentes estatales no significa que las empresas privadas estén a salvo de las APT. Este tipo de agentes de amenaza son sigilosos porque hackear otra agencia gubernamental o empresa de servicios públicos es costoso y consume mucho tiempo. Las APT suelen apuntar primero a organizaciones privadas como un paso hacia el acceso a entidades más grandes.

**Puntos de acceso**

Cada agente de amenaza tiene una motivación específica a la hora de establecer los activos de una organización como objetivo. Mantenerlos alejados requiere más que conocer sus intenciones y capacidades. También es importante reconocer los tipos de vectores de ataque que utilizarán.

En su mayor parte, los agentes de amenaza obtienen acceso a través de una de estas categorías de vectores de ataque:

* **Acceso directo**, que hace referencia a instancias en las que tienen acceso físico a un sistema.
* **Medios extraíbles**, que incluyen hardware portátil, como unidades USB.
* **Plataformas de redes sociales** que se utilizan para la comunicación y el intercambio de contenido.
* **Correo electrónico**,incluidaslas cuentas personales y comerciales.
* **Redes inalámbricas** en las instalaciones.
* **Servicios en la nube** que por lo general son proporcionados por organizaciones de terceros.
* **Cadenas de suministro,** como proveedores externos que pueden presentar una puerta trasera en los sistemas.

Cualquiera de estos vectores de ataque puede proporcionar acceso a un sistema. Reconocer las intenciones de un actor de amenazas puede ayudarte a determinar a qué puntos de acceso podrían apuntar, y cuáles podrían ser sus objetivos Por ejemplo, es más probable que los trabajadores remotos presenten una amenaza por correo electrónico, que una amenaza de acceso directo.

**Conclusiones clave**

Defender una superficie de ataque comienza con pensar como atacante. Como profesional de la seguridad, es importante entender *por qué* alguien representaría una amenaza para los activos de una organización. Esto incluye reconocer que no todos los agentes de amenaza pretenden causar daño intencionadamente.

Además, es muy importante reconocer las formas en que un agente de amenaza podría obtener acceso a un sistema. Hacer coincidir las intenciones con los vectores de ataque es una habilidad invaluable para desarrollar la mentalidad de atacante.