Pentesting: Hacking ético en la banca

El sector bancario es consciente de que, a medida que avanza en su proceso de digitación, es esencial el mantenimiento de unos altos estándares de ciberseguridad. Ante este reto, los bancos están cambiando su estrategia. La mejor manera de estar preparado para poder dar una respuesta a los potenciales ciberataques en conocer cómo se comportaría un hacker informático. Así, crece el uso en el sector bancario del "pentesting" o el "hackeo ético", como estrategia de seguridad.

Los bancos son las entidades que más ataques cibernéticos reciben anualmente. Algunos estudios realizados por el propio sector apuntan a que cerca del 67% de las instituciones financieras sufren algún tipo de ataque informático (hacking o malware) a lo largo del año[1]. Además se constata que los cibercriminales se han vuelto más sofisticados, como demuestra la proliferación de ataques coordinados[2].

Para dar respuesta a este reto, el sector bancario comienza a utilizar nuevas estrategias de defensa como el "pentesting" o hackeo ético. Consisten en el desarrollo de un plan de seguridad que tiene por objeto la detección de las vulnerabilidades de un sistema informático. Para ello, se atacan los propios sistemas deliberadamente, pero de forma controlada. El objetivo es analizar los resultados del ataque simulado para detectar las debilidades del sistema. El fundamento de la estrategia parte de la premisa de que para garantizar la seguridad de un sistema es necesario ponerse en la piel de los hackers. Así, la fase inicial de cualquier

[1] Modern Bank Heists: The Bank Robbery Shifts to Cyberspace. CarbonBlack. https://www.carbonblack.com/resources/threat-research/modern-bank-heists-the-bank-robbery-shifts-to-cyberspace/#form

[2] Seven UK banks targeted by co-ordinated cyber attack. Financial Times. https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb

"pentesting" consiste en secuestrar el sistema y todos sus datos para intentar explotar las vulnerabilidades de la misma manera que lo haría un hacker externo.

Además, el sector bancario también está comenzando a combinar esta estrategia con la inteligencia artificial (*machine learning*). Con ello se pretende analizar los resultados del ciberataque simulado para inferir los patrones de comportamiento algorítmico de los ciberatacantes reales.

Aunque el uso de dicha estrategia no asegura un nivel de protección infalible, lo que sí que que se observa es que aquellas entidades que han utilizado el hackeo ético como forma activa de defensa han mejorado la seguridad de sus sistemas y la posibilidad de dar respuesta rápida a los ciberataques.