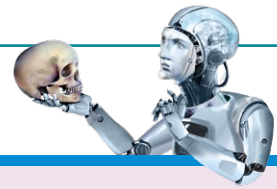
CAVILACIONES SEGURAS



Pruebas basadas en amenazas: hacia una mayor resiliencia dirigida

Hace ya muchas lunas, cuando la ciberseguridad se llamaba seguridad informática y los responsables de dicha seguridad andaban muy lejos de la dirección de su compañía, y más aún de su consejo de administración, algunos pioneros, con quien tuve la suerte de trabajar, proponían que el presupuesto de seguridad fuera a prevenir aquellos ataques que se veían en la industria, en vez de intentar proteger a la organización de todo ataque posible.

Protegernos de todo y en todo momento, si bien es una bonita quimera, no es en absoluto viable, tanto desde el punto de vista económico, como desde el punto de vista estratégico.

En el sector financiero, hace menos de una década de la llegada al campo de la seguridad tecnológica de teorías militares de defensa basadas en el análisis de las amenazas que despliega el enemigo.

Los proveedores nacionales de informes de inteligencia y de pruebas de intrusión tienen una oportunidad de oro para satisfacer con profesionalidad y calidad un mercado que sólo va a poder crecer en los próximos años. Les invito a internacionalizarse y a innovar en este campo, que ahora empieza a dar sus primeros pasos.

Así, en 2014, el Banco de Inglaterra propuso CBEST, un programa de evaluación de seguridad basado en amenazas (concepto conocido con las siglas en inglés TLPT: "threat-led penetration testing"). En 2016, se publicaban las guías prácticas de CBEST. En 2017, la autoridad monetaria de Hong Kong publicaba iCAST ("intelligence-led Cyber Attack Simulation Testing) y el Banco Central de Holanda hacía lo mismo con TIBER-NL ("Threat Intelligence Based Ethical Red teaming"). Finalmente, en 2018, la Asociación Bancaria de Singapur (ABS) publicó AASE ("Adversarial Attack Simulation Exercises"). En mayo de 2018 el Banco Central Europeo publica TIBER-EU, un marco de pruebas de seguridad, en el entorno de producción, basado en dos elementos esenciales: un informe de inteligencia sobre amenazas y unas pruebas de intrusión guiadas por dicho informe de amenazas. TIBER prevé que ambos elementos sean realizados a través de proveedores externos a la entidad financiera. Todas están propuestas van dirigidas a aumentar la resiliencia tecnológica del sector financiero.

En enero de 2022, el Banco de España publicó la guía de implementación de TIBER-ES, en línea con las directrices de TIBER-EU. La propia guía recuerda que estas pruebas están dirigidas a entidades significativas o sistémicas, ya sean bancos, aseguradoras, gestoras de activos o infraestructuras críticas de mercado, todas ellas con un grado de madurez suficiente como para poder embarcarse en este tipo de evaluación. En Europa, la implementación de cada uno de los TIBER nacionales va a suponer un ahorro de esfuerzos, ya que el objetivo es garantizar el reconocimiento de estas pruebas en todas los Estados que adopten el marco TIBER-EU.

El elemento adicional que puede suponer el despegue de estas pruebas es la próxima aprobación del reglamento europeo sobre la resiliencia operativa digital del sector financiero (conocido por las siglas DORA), donde probablemente se exigirán este tipo de pruebas de seguridad a las entidades financieras significativas.

Los proveedores nacionales de informes de inteligencia y de pruebas de intrusión tienen aquí una oportunidad de oro para satisfacer con profesionalidad y calidad un mercado que sólo va a poder crecer en los próximos años. Desde esta columna les invito a internacionalizarse y a dedicar partidas importantes de su presupuesto a innovar en este campo, que ahora empieza a dar sus primeros pasos.

Concluyo enumerando las principales recomendaciones que proponían en 2021 los proveedores de ciberinteligencia en una encuesta realizada en el entorno CBEST. Toda una lista de ideas a desarrollar en un continuo proceso de innovación: creación de un marco global de pruebas TLPT a nivel mundial que permita a las marcas financieras globales una reducción de costes regulatorios; adaptación de los informes de inteligencia a las necesidades reales de cada entidad evaluada; posibilidad de "pivotar" en las pruebas de intrusión, tal y como haría un atacante real, así como inclusión de técnicas activas de reconocimiento de vulnerabilidades en la creación del informe de inteligencia; creación de una versión con pruebas más ligeras para entidades más pequeñas; un papel más relevante del denominado equipo morado ("the purple team", formado por atacantes y defensores) para que la prueba realizada sea una verdadera oportunidad de aprendizaje para el equipo defensor ("the blue team") y, finalmente, una mayor cooperación con los servicios de inteligencia nacionales.

Alberto Partida
Experto en Ciberseguridad
https://linkedin.com/in/albertopartida