Comentario THIBER:

Reino Unido: ¿nuevo enfoque para la ciberseguridad nacional?

AUTOR: Por Enrique Fojón, sub-director de THIBER

Fuente: UK Ministry of Defense.

En 2016, tras cuatro años, un exhaustivo plan de implementación y casi 1.000 millones de euros invertidos, el gobierno conservador de David Cameron hacía un balance positivo de los logros alcanzados tras la culminación de la primera Estrategia Nacional de ciberseguridad. Sin embargo, Londres también reconocía que esta inversión no había sido suficiente.

En consecuencia, a finales de 2016 se aprobó la segunda Estrategia Nacional de Ciberseguridad (2016-2021) que, partiendo de los hitos alcanzados por la primera, contaba con un presupuesto aproximado de 2.200 millones de euros para consolidar el incipiente Sistema Nacional de Ciberseguridad.

Al igual que esta ocurriendo en la inmensa mayoría de las estrategias nacionales de ciberseguridad aprobadas por nuestros principales socios y aliados, la del Reino Unido es intervencionista y concede al gobierno de Londres un papel protagonista en la dirección y gestión de la ciberseguridad nacional. La estrategia pretende que en 2021 se haya consolidado: el desarrollo

«La Estrategia Nacional de Ciberseguridad del Reino Unido es intervencionista y concede al gobierno de Londres un papel protagonista en la dirección y gestión de la ciberseguridad nacional”

de un conjunto de políticas públicas; cambios organizativos, donde se incluye el ya constituido National Cyber Security Centre’s (NCSC’s) y la implementación de los Active Cyber Defence (ACD); implementación de tecnologías nacionales y dinamización de la industria tecnológica del país.

Sin embargo, la ausencia de métricas hace muy difícil cuantificar el retorno de la inversión del gobierno británico y cuál ha sido la mejora real de la ciberseguridad nacional, máxime cuando la dependencia tecnológica del país es cada vez mayor y el tipo de riesgos y amenazas cibernéticas se multiplican año tras año.

Es por ello que el gobierno de Londres está ya trabajando en la nueva estrategia nacional de ciberseguridad, que deberá cubrir el periodo 2021-2026. Desde 2011 se han identificado muchas lecciones y aprendido la inmensa mayoría de ellas. En la actualidad, el gobierno está analizando:1) el futuro rol del sector privado del Reino Unido, máxime cuando la inmensa mayoría de las infraestructuras críticas del país están en sus manos; 2) políticas incentivadoras, que permitan a la industria y ciudadanos implementar estándares y buenas prácticas en materia de ciberseguridad; 3) Evaluar los riesgos asociados a la globalización de la tecnología, el caso de Huawei y el 5G son solo un ejemplo; y 4) analizar la capacidad industrial del Reino Unido en materia de ciberseguridad, máxime cuando el ecosistema de start-ups del país no ha alcanzado el éxito esperado.

En definitiva, el Reino Unido se encuentra inmerso en un proceso de reflexión donde el rol de la industria nacional de ciberseguridad resulta esencial.