LINCE, certificación de seguridad para todos los públicos

Históricamente los fabricantes de productos de seguridad IT han visto la certificación como una exigencia del guión para acceder a determinados mercados que provocaba todo tipo de inconvenientes en los procesos de desarrollo sin aportar verdadero valor. Europa ha sido consciente de este problema y los diferentes países de la Unión están dando respuestas para mejorar esta situación. España ya lo ha hecho y su respuesta se llama LINCE: una certificación ligera, enfocada en el análisis de vulnerabilidades y con una duración y coste acotados.

José Ruiz / Javier Tallón

Antecedentes: El Catálogo CPSTIC

El pasado mes de marzo, publicábamos en esta misma revista un artículo acerca de la creación por parte de la administración del Catálogo de Productos STIC (CPSTIC), un catálogo de referencia para la adquisición de productos TIC en organismos públicos afectados por el Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para la adquisición de productos en organismos que manejen información clasificada.

Este Catálogo se compone del Listado de Productos Cualificados: productos que tienen certificadas sus funcionalidades de seguridad y, por lo tanto, son aptos para ser utilizados en sistemas afectados por el ENS que hayan sido etiquetados como Categoría ALTA por requerir un nivel alto de seguridad en cualquiera de sus dimensiones (Confidencialidad, Disponibilidad, Integridad, Trazabilidad y Autenticidad).

Este esfuerzo realizado por el CCN permite desde entonces a la administración española la adquisición de productos certificados con mayor seguridad y sencillez, siendo una herramienta clave para el futuro de la lucha contra las ciberamenazas.

Sin embargo, quedaba una pregunta pendiente de contestar: ¿Qué sucede con aquellos sistemas de Categorías BAJA o MEDIA? ¿No es aplicable el catálogo en esos casos?

Certificaciones: ¿Los malos de la película?

La experiencia ha demostrado que la normativa internacional (Common Criteria) en cuanto a certificación es una metodología muy valiosa, y por ello es la puerta de entrada al Catálogo CPSTIC para categoría ALTA. Por un lado, es tremendamente potente, contemplando la ciberseguridad desde múltiples ángulos y proporcionando garantía no solo en cuanto a los componentes más técnicos, sino también desde otras muchas perspectivas como el ciclo de vida, el entorno de desarrollo, o la documentación de diseño. Además, es versátil y flexible, siendo aplicable a todo tipo de productos y permitiendo elegir entre distintos niveles de garantía en función de la criticidad del producto. Todo esto sin contar con el reconocimiento internacional.

Por otro lado, y comparando un servicio de *hacking* ético con una evaluación formal de un producto, en ambos casos los resultados dependerán de las capacidades técnicas del evaluador en cuestión; pero la presencia de un tercero (en España el Centro Criptológico Nacional para la certificación Common Criteria o LINCE), que vele por asegurar la calidad de los resultados, es un valor que no puede ser despreciado.

Sin embargo, Common Criteria no está exenta de problemas; en primer lugar, porque es demasiado lenta, incluso en los niveles más bajos de garantía; una certificación requiere de al menos 6 meses de duración, que en ocasiones es dedicado en gran parte a la creación de "papel" para "cumplir el expediente", sin contar además con la dificultad técnica para cumplir el estándar debido, entre otras cosas, a la excesiva rigidez del mismo. Esto supone unos costes muy elevados que hacen que este tipo de certificaciones solo sean accesibles a grandes empresas, cuando, como todos sabemos, España es un país de pymes.

En un mundo donde las actualizaciones de software pueden llegar a ser prácticamente diarias debido a la prevalencia de metodologías ágiles, está claro que Common Criteria no es capaz de responder de manera adecuada a las necesidades actuales de la industria ni de los ciudadanos, que quieren disfrutar las últimas innovaciones tecnológicas sin tener que renunciar a las garantías que ofrece un producto que ha sido testeado de manera metódica e independiente.

El panorama europeo

La situación vivida en España no es distinta a la que podemos encontrar en otros países a nivel europeo, provocando dos respuestas diferentes en la búsqueda de una alternativa eficiente a Common Criteria.

Por un lado, mediante la creación de esquemas privados sectoriales fuertemente basados en Common Criteria, pero poniendo el foco en los aspectos técnicos y reduciendo la carga documental y los tiempos de espera y ejecución (como EMVco para pago o como Felica y MiFare para transporte).

Por otro lado, mediante la creación de metodologías de evaluación ligeras dentro de los esquemas de certificación de cada país, como BSPA (*Baseline Security Product Assessment*) en Holanda o CSPN (*Certification de Sécurité de Premier Niveau*) en Francia, que lleva funcionando desde hace ya varios años.

Estos hechos coinciden con la aparición a nivel europeo del *European Cybersecurity Certification Framework*, sobre el que se concede a ENISA mandato permanente y que busca la creación de un nuevo esquema común a todos los países de la Unión, contemplando tres niveles de garantía: básico, sustancial y alto.

LINCE, la Certificación Nacional Esencial de Seguridad de productos TIC creada por el CCN, no es un sustituto de Common Criteria: su objetivo es ofrecer una garantía de seguridad para los fabricantes y consumidores a un nivel más asequible en tiempo, esfuerzo y dinero.

¿Qué es LINCE?

LINCE es una metodología ligera de evaluación y certificación de productos TIC, creada por el Centro Criptológico Nacional, de alcance nacional (por el momento), basada en los principios de Common Criteria y orientada al análisis de vulnerabilidades y los test de penetración. Los puntos fuertes de LINCE sobre certificaciones más robustas consisten principalmente en un menor esfuerzo, duración y coste para el fabricante. Sin embargo, por la forma en la que se aplica, también permite prestar más atención a los puntos críticos de cada producto, dando más peso a las pruebas concretas y prácticas que combatan amenazas reales que a documentación densa o test de funcionalidad exhaustivos.

LINCE viene a cerrar el círculo de los problemas expuestos en los párrafos anteriores:

– Alineando España con las tendencias en certificación europeas, que buscan centrar el esfuerzo de evaluación en el análisis de vulnerabilidades.

– Proporcionando un marco de certificación ágil con un esfuerzo y duración claramente acotados en concordancia con las metodologías de desarrollo modernas.

– Permitiendo la creación de un catálogo para niveles BAJO y MEDIO que dé respuesta a las necesidades de seguridad de los sistemas de la administración bajo dichos niveles de amenaza.

LINCE no es un sustituto de Common Criteria, su objetivo es ofrecer una garantía de seguridad para los fabricantes y consumidores a un nivel más asequible en tiempo, esfuerzo y dinero.

Actualmente, LINCE está directamente orientada a la evaluación y certificación de productos de seguridad TIC para su inclusión en el catálogo CPSTIC para niveles medio o bajo del ENS conforme a los establecido en las guías CCN-STIC-107 y CCN-STIC-141, aunque también se puede emplear para la realización de Evaluaciones STIC complementarias conforme a lo especificado en las guías CCN-STIC-106 y CCN-STIC-140, las cuales pueden ser usadas cuando el producto ya ha sido certificado pero el alcance de la evaluación no era el requerido en el catálogo.

Uno de los aspectos más interesantes de LINCE es que no requiere de una costosa preparación por parte del fabricante. Simplemente se ha de entregar el producto a evaluar, el entorno de ejecución, las guías de uso del producto y una declaración de seguridad (sin el formalismo requerido en Common Criteria) para determinar la funcionalidad de seguridad que será objeto de la evaluación. Este es uno de los puntos más importantes de LINCE porque **permite que multinacionales cuyos centros de desarrollo estén ubicados en el extranjero, puedan optar a entrar en el catálogo** sin necesidad de involucrar a la matriz activamente en el proceso, lo que conllevaba mucho esfuerzo y retrasos.

El proceso de certificación. ¿Cómo entrar en el catálogo?

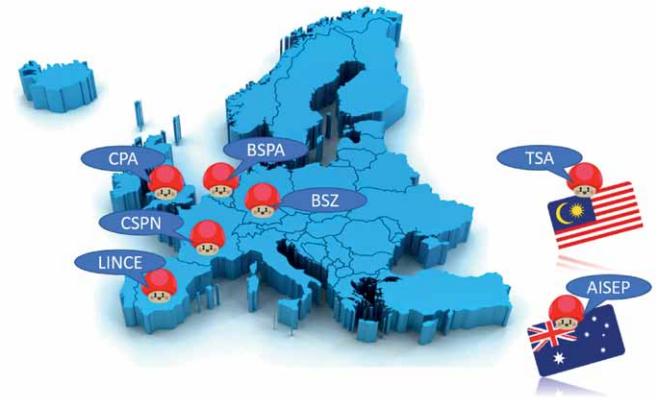
El primer paso es la redacción de una declaración de seguridad por parte del fabricante, donde se describe la funcionalidad de seguridad del producto. Esta descripción tiene un carácter informal y se realiza siguiendo la plantilla CCN-LINCE-003, lo cual facilita enormemente la tarea.

Esa declaración de seguridad será revisada por el personal del CCN encargado del catálogo CPSTIC para verificar que cumpla con los requisitos definidos para una tipología de productos dentro de los definidos en la guía CCN-STIC 140: "Taxonomía de referencia para productos de Seguridad TIC". Una vez se reciba la aprobación, se podrá iniciar el proceso.

Al igual que el resto de certificaciones gestionadas a través del Centro Criptológico Nacional, el proceso comienza con el envío de un formulario de solicitud de certificación al que se debe adjuntar la Declaración de Seguridad.

Además, el fabricante deberá poner a disposición del laboratorio un entorno de funcionamiento válido, el producto y los manuales del producto a evaluar.

Toda esta información (a excepción si acaso de la ST) ya suele estar en poder del fabricante en cualquier proceso de desarrollo, requiriendo por tanto un esfuerzo mínimo para poner en marcha el proceso y evitando así la tediosa tarea de generación de documentación *ad hoc* que exigía Common Criteria.



Es de esperar que todas las certificaciones ligeras europeas sean recogidas bajo el paraguas del nuevo Framework para el nivel de garantía sustancial, permitiendo el reconocimiento de las mismas en los diferentes países adscritos al mismo. De hecho, ya se ha lanzado un estudio de viabilidad para la creación de una metodología ligera a nivel europeo, que podría ser la base de esquemas de certificación verticales (IoT, Automoción, Industria, etc.) que se crearán en los próximos años.

A partir de ese momento, la metodología fija una duración máxima de 8 semanas para la evaluación, con un esfuerzo acotado en 25 días/hombre.

Si el producto supera el proceso de evaluación de manera satisfactoria, se finalizará con la emisión de un certificado por parte del CCN que demuestre que un producto cumple con los requisitos de seguridad especificados en su declaración de seguridad.

¿Qué nos depara el Futuro?

Nadie sabe qué ocurrirá en el futuro, pero es de esperar que todas las certificaciones ligeras europeas sean recogidas bajo el paraguas del nuevo Framework para el nivel de garantía sustancial, permitiendo el reconocimiento de las mismas en los diferentes países adscritos al mismo. De hecho, ya se ha lanzado un estudio de viabilidad para la creación de una metodología ligera a nivel europeo. Esta futura metodología podría ser la base de esquemas de certificación verticales (IoT, Automoción, Industria, etc..) que se crearán en los próximos años.

Conclusión

La administración, la industria y los usuarios finales estamos de enhorabuena. Por fin disponemos de una herramienta ágil y eficaz para verificar la seguridad de nuestros productos con la tranquilidad de estar siguiendo una metodología alineada con las iniciativas europeas y amparada por un esquema de certificación que garantiza la calidad de los trabajos realizados.

LINCE permite a los fabricantes hacerse cargo por sí mismos de preparar la documentación y todo lo necesario para iniciar el procedimiento permitiendo la entrada de las pymes y las filiales nacionales de las grandes multinacionales cumpliendo con los requisitos establecidos por CCN para entrar en el catálogo CPSTIC.

Es el momento de que los fabricantes de seguridad se suban al carro de la certificación y el ejemplo dado por la administración española para salvaguardar la seguridad de los ciudadanos se expanda a otros sectores clave, como las infraestructuras críticas. ■

José Ruiz
CTO - Director de Tecnología
jruiz@jtsec.es

Javier Tallón
COO – Director de Operaciones
jtallon@jtsec.es

JTSEC