>> Jorge Dávila

¿Para cuándo la certificación generalizada de productos?

Las brechas de seguridad, las exanguinaciones de datos personales y sensibles y la proliferación de fallos de siempre en los sistemas que día a día utilizamos siguen siendo continuas. La sociedad está decidida a lanzarse a una Economía Digital plena y no estaría mal que alguien, que muchos, de forma independiente y responsable, echaran un vistazo a la seguridad y corrección de lo que todos los días utilizamos. Es el tema de la Certificación de Productos TIC y conviene echar un vistazo a lo que está ocurriendo, a ver si así entendemos qué esta pasando.

A finales del pasado mes de julio se supo que el grupo médico más grande de Singapur, SingHealth, había sido víctima de una brecha en su seguridad que había permitido la fuga de información personal (historiales clínicos y medicación dispensada) de 1,5 millones de pacientes que utilizaron sus servicios entre los meses de mayo de 2015 y julio de 2018. Las investigaciones preliminares confirman que este ataque ha sido deliberado, dirigido y bien planificado, y no parece ser obra de hackers eventuales o bandas criminales. Por lo visto, el objetivo eran los registros médicos del Primer Ministro Lee Hsien Loong[1], así como información sobre las medicinas que toma.

El desastre comenzó como siempre, en una única estación de trabajo colocada en el *front-end* de la infraestructura y desde allí los atacantes lograron obtener credenciales privilegiadas de acceso a la base de datos y con ello a su botín.

Por otra parte, a mediados del mismo mes de julio, una organización de consumidores (FACUA) informa a Telefónica que tiene un boquete inmenso abierto en sus sistemas de atención al cliente. Un error de programación de sus sistemas web dejó expuestos millones de datos de sus clientes aunque fuese resuelto en pocas horas. Se trataba de una debilidad del sistema que permitía a cualquiera sin excesivos conocimientos técnicos, obtener los datos de miles o millones de clientes (DNI, lugar de residencia, llamadas hechas y recibidas, consumo, datos de facturación).

Para acceder a los datos de otros clientes, los usuarios sólo tenían que estar conectados al sistema, acceder a los datos de su factura y cambiar levemente la URL que le ofrecía el sistema para ver sus datos, y con ello ver los datos de alguien que no era él o ella. Lo más curioso es que esto resuena en la memoria colectiva y sólo hay que retrotraerse al incidente LexNet[2] del Ministerio de Justicia[3] (27 de julio de 2017) para ver que a Telefónica le pasó exactamente lo mismo que entonces.

Este tipo de errores ya estaban presentes en las webs de hace treinta años; el tiempo ha pasado, la miniaturización se ha zambullido en el vacío atómico, pero seguimos pudiendo decirle a una base de datos de una gran compañía que nos de cualquier cosa que se nos ocurra con sólo cambiarle la URL que nos dan. Está claro que, tristemente, en la informática hay cosas que permanecen.

Abrumados por este padecer de errores recurrentes, aparece un documento, un borrador[4] del Presidente al Consejo de la Unión Europea, en el que se vuelve a escribir sobre lo que son los cometidos de ENISA[5] –fundada allá por 2004–; pero en realidad se trata de la futura Ley de Seguridad Cibernética de la Unión Europea que todavía está en plena gestación.

En la mayoría de los casos en el desarrollo de software no hay más que un burdo ensayo funcional que sólo comprueba que el nuevo constructo software-hardware hace lo que el departamento de márquetin llama "negocio". Cuanto más corto es el tiempo de vida esperado para un producto TIC, menos es el interés de las empresas en cuidar que sea seguro e incluso correcto.

La certificación en informática

Lo más interesante de ese borrador es la segunda parte de su título, "*and*

[1] Ver https://en.wikipedia.org/wiki/Lee_Hsien_Loong

[2] Ver https://es.wikipedia.org/wiki/Lexnet

[3] Ver https://www.elconfidencial.com/tecnologia/2017-07-27/lexnet-justicia-sistema-telematico_1421771/

[4] Doc 9350/18 : Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

[5] Ver https://www.enisa.europa.eu/

Communication Technology Cybersecurity Certification" ¿Qué es eso de la certificación en informática?

Que sigan apareciendo hoy errores en el desarrollo de software que ya se veían hace 30 años, tiene su origen en que, como entonces, el software de ahora pasa a producción sin que lo haya verificado nadie. Sé que algunos dirán que eso no es así, que sus Departamentos de Control de Calidad (cuando los hay) se preocupan de que lo que entra en producción sea lo mismo que los diseñadores idearon en un principio; sin embargo, nadie se ha preocupado realmente por la seguridad de lo que se ideó, de lo que se implementó o incluso, de lo que se está utilizando.

En la mayoría de los casos no hay más que un burdo ensayo funcional que sólo comprueba que el nuevo constructo software-hardware hace lo que el departamento de márquetin llama "negocio". Cuanto más corto es el tiempo de vida esperado para un producto TIC, menos es el interés de las empresas en cuidar que sea seguro e incluso correcto, y cada día vivimos más acelerados.

Otro de los vicios de nuestro escenario TIC actual es que sólo sean departamentos de técnicos o de calidad de las empresas promotoras del producto las que se encarguen de evaluar la calidad, corrección y seguridad de lo que esas mismas empresas están desarrollando o ellas mismas han diseñado. Nunca ha sido bueno para la claridad ser juez y parte, y tampoco lo es para la seguridad. Es en este punto en el que surge la necesidad de la "Certificación de productos"[6].

Otro vicio de nuestro escenario TIC actual es que sólo sean departamentos de técnicos o de calidad de las empresas promotoras del producto las que se encarguen de evaluar la calidad, corrección y seguridad de lo que esas mismas están desarrollando o han diseñado. Nunca ha sido bueno para la claridad ser juez y parte, y tampoco lo es para la seguridad.

La certificación de productos

La certificación de cualquier producto es un proceso en el que a dicho producto se le somete a ciertos ensayos sobre sus prestaciones y su calidad. Si los resultados obtenidos indican que el producto cumple con el criterio de cualificación establecido mediante contratos, regulaciones sectoriales o especificaciones en general (*certification schemes*), entonces el producto recibe el correspondiente "Certificado".

El que hace esas pruebas nunca es la empresa promotora del producto, no puede tener intereses de ningún tipo con ella, y debe ser un ente reconocido internacionalmente como Laboratorio Evaluador válido[7] dentro del esquema de certificación del que se trate.

La certificación de productos es obligatoria en sectores industriales sensibles en los que un fallo puede tener serias consecuencias y afectar negativamente a la salud y calidad de vida de la persona o personas que utilicen ese producto. Ejemplos bien conocidos son el sector aeronáutico y aeroespacial, la industria alimentaria, la farmacéutica, la de la Salud, la de sustancias peligrosas, etc.

El proceso de certificación suele hacerse en cuatro etapas:**1)** Ensayos del producto y obtención de resultados, **2)** Evacuación de si esos resultados cumplen el criterio de evaluación, **3)** Decisión de conceder o no la certificación, y **4)** Vigilancia de si el producto sigue cumpliendo en el tiempo con el criterio de certificación una vez que ha conseguido el certificado. Prácticamente ninguno de los productos y sistemas TIC que "agilizan" nuestro Occidente han pasado por ninguno de esos pasos.

Algunos sectores como el financiero, espoleados por la férrea normalización a la que se someten, han empleado cierto esfuerzo en "normalizar" muchas de sus acciones (por ejemplo, medios de pago), pero en el sector de la obtención y distribución de información a través de plataformas Web,la certificación es desconocida y no se la espera.

Prácticamente ninguno de los productos y sistemas TIC que "agilizan" nuestro Occidente han pasado por ninguno de los cuatro pasos necesarios para un proceso de certificación, y los sistemas de certificación industrial que nacieron en el siglo XX no pueden atender el dinamismo actual y futuro de las TIC y todo lo que lleva asociado.

Dado que cada día son más graves las consecuencias que el mundo Web y todo lo construido sobre él tienen sobre el ciudadano y la sociedad actual, empieza a ser necesario obligar a algún tipo de certificación, homologación o ensayo de al menos su seguridad, a todo ese "tejido" (*fabric*) con el que Administraciones y empresas se relacionan con ciudadanos y clientes, o incluso entre personas individuales (Ashley Maddison[8], Tinder[9], etc.)

Dado que las tecnologías TIC lo empapan todo, la UE pretende agilizar la certificación de productos de modo que ciudadanos y empresas puedan obtener productos cuyas características estén certificadas por alguien independiente y confiable y, si es posible, con los mismos patrones en todos los estados miembros de la UE.

[6] Ver https://en.wikipedia.org/wiki/Product_certification

[7] Ver ISO/IEC Guide 65 de 1996, e ISO/IEC 17011 de 2004.

[8] Ver https://en.wikipedia.org/wiki/Ashley_Madison

[9] Ver https://en.wikipedia.org/wiki/Tinder_(app) y https://en.wikipedia.org/wiki/Hookup_culture

La evaluación Common Criteria

A la luz de este discurso podría parecer que no existe infraestructura para conseguir evaluar los dispositivos y servicios que utilizamos, y la realidad es todo lo contrario. Existen numerosos esquemas de certificación nacionales e internacionales centrados específicamente en las tecnologías y productos TIC. Uno de los más conocidos es el **Common Criteria**[10] **Evaluation and Validation Scheme** (**CCEVS**) del gobierno de los EEUU que está administrado por la National Information Assurance Partnership (NIAP). Sus objetivos son evaluar las funcionalidades de seguridad de las tecnologías de la información respecto a un único estándar internacional.

La evaluación Common-Criteria (CC) es un proceso lento y caro, y lo que obtiene el contratante a cambio no es necesariamente un producto más seguro y sus clientes lo saben. La evaluación CC se centra principalmente en la corrección de lo establecido en la documentación de evaluación y no tanto en pruebas concretas de la seguridad del producto o la corrección técnica del mismo.

De todos los niveles de evaluación, sólo en el último y altamente infrecuente, EAL7, no se exige el análisis del código. El esfuerzo y el tiempo necesario para preparar las evidencias documentales que se van a evaluar es enorme y para cuando el proceso se ha completado, la evaluación del producto está casi siempre obsoleta.

Algunos incluyen como crítica al esquema Common Criteria que discrimina, por su forma de proceder, al software libre y al *open-source* (FOSS) ya que su metodología está inspirada en el modelo tradicional en cascada[11] del desarrollo de software. En cualquier caso, una vez certificados los productos el certificador no controla activamente que sigue cumpliéndose con el tiempo lo que el certificado manifiesta. Varias versiones de Windows Server 2003 y Windows XP fueron certificadas CC, pero los parches de seguridad para tapar vulnerabilidades descubiertas posteriormente invalidan, de facto, el certificado original.

Algo se mueve en la certificación

Algo debe estar cambiando cuando países como Francia, Alemania y España[12] se mueven hacia el establecimiento de nuevos esquemas de certificación que sean: 1) más livianos en su ejecución sin que ello degrade el valor semántico del certificado; y 2) ampliar el conjunto de entes acreditados capaces de hacer las evaluaciones favoreciendo así la sana competencia comercial entre ellos. No es razonable aceptar que el número de laboratorios y agentes evaluadores sea escaso y pueda vivir recluido en el pequeño nicho de mercado donde la certificación es obligatoria. Esquemas como los actuales dejan desprotegida a toda la sociedad que ya lleva las tecnologías TIC en las venas.

Nuestra sociedad necesita urgentemente que se evalúen y certifiquen todos los dispositivos, sistemas y procesos relacionados con la información y quizás por ello, tímidamente, la Unión Europea lo ha incluido explícitamente en su "Cybersecurity Act". Sin embargo es necesario cambiar los modos de certificar y hacerlos más ágiles y continuos. Los sistemas de certificación industrial que nacieron en el siglo XX no pueden atender el dinamismo actual y futuro de las TIC y todo lo que lleva asociado.

Por el momento el cliente, tanto si es empresa como si es ciudadano, usuarios finales a fin de cuentas, sólo pueden vanamente confiar en los fabricantes e integradores, y con ello está en sus manos, indefenso, como un cordero esperando en la cola a que le pase algo. Ese día, ni el fabricante, ni los certificados, ni aquellos que los emitieron vendrán a ayudarle ni asumirán ninguna responsabilidad en su desgracia. Está tardando ya el día en que esto ya no sea así. ■

La evaluación Common Criteria es un proceso lento y caro, y lo que obtiene el contratante a cambio no es necesariamente un producto más seguro y sus clientes lo saben. La evaluación CC se centra principalmente en la corrección de lo establecido en la documentación de evaluación y no tanto en pruebas concretas de la seguridad del producto o la corrección técnica del mismo.

No es razonable aceptar que el número de laboratorios y agentes evaluadores sea escaso y pueda vivir recluido en el pequeño nicho de mercado donde la certificación es obligatoria. Esquemas como los actuales dejan desprotegida a toda la sociedad que ya lleva las tecnologías TIC en las venas.

[10] Ver https://en.wikipedia.org/wiki/Common_Criteria

[11] Ver https://en.wikipedia.org/wiki/Waterfall_model

[12] Ver https://securmatica.com/index.php/programa/securmatica-2018-programa-modulo-1

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es