ARI 91/2019
10 de septiembre de 2019

Ciberseguridad: construyendo cadenas de suministros seguras y de confianza

Ana I. Ayerbe | Directora del Área de Negocio TRUSTECH de Tecnalia | @AnaAyerbe

Tema

Mantener la confianza en el mundo digital e hiperconectado implica desarrollar la ciberseguridad desde el diseño y por defecto, tanto en el ciclo de vida de desarrollo de sistemas como a lo largo de la cadena de suministro.

Resumen

La economía y la sociedad digitales en las que estamos inmersos dependen de la confianza en el buen funcionamiento de los sistemas y servicios digitales, una confianza que puede verse minada por los ciberataques, que afectan a su seguridad, privacidad y fiabilidad. Este ARI describe la necesidad de prestar mucha atención a la ciberseguridad tanto durante el ciclo de vida de desarrollo de los sistemas como en la cadena de suministro, las dificultades que encuentran las empresas, ciudadanos y Administraciones para hacerlo y las acciones que pueden llevarse a cabo desde las diferentes instituciones para facilitarla y crear una cultura de la ciberseguridad desde el diseño y por defecto.

Análisis

La Unión Europea (UE) acaba de identificar la ciberseguridad como una de las "cadenas de valor estratégicas" que potenciar en Europa, reconociendo su relevancia más allá del ámbito tecnológico y reflejando la necesidad de que las Administraciones y las industrias de los Estados miembros coordinen sus acciones e inversiones para asegurar que la UE se convierta en un líder industrial mundial en este ámbito[1].

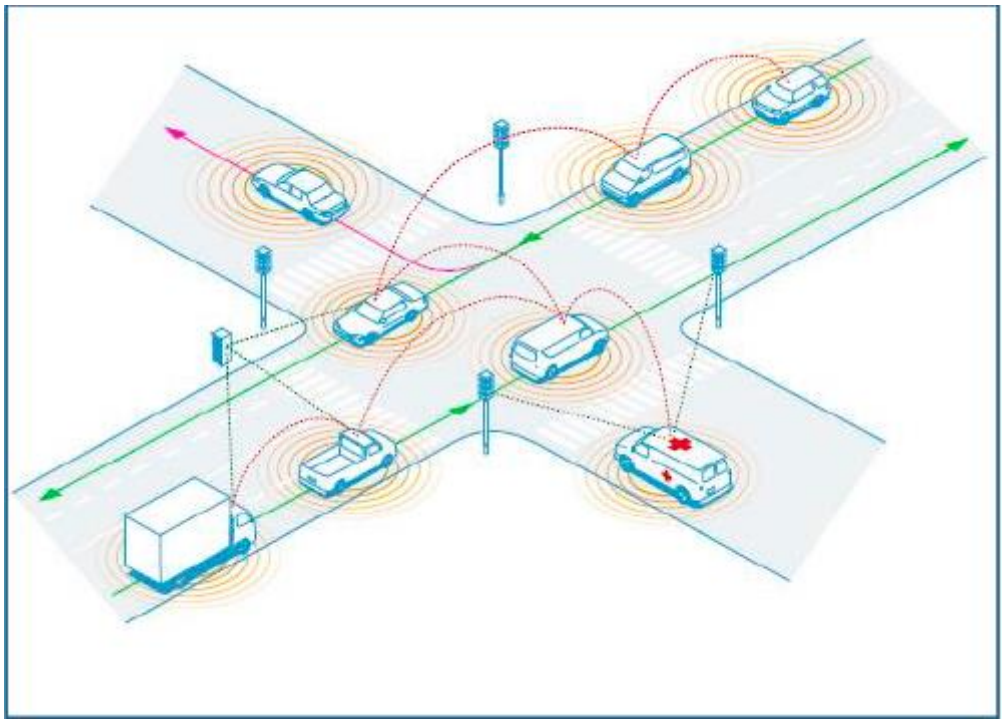
La razón por la que la UE considera que hay que proteger y potenciar la cadena de valor de la ciberseguridad es porque garantiza el desarrollo de la economía digital. Vivimos en un mundo digital e hiperconectado en el que las personas incorporamos cada vez más inteligencia y conectividad a objetos cotidianos (móviles, frigorífico, televisión o coche, entre otros), las Administraciones Públicas aumentan sus servicios digitales y las máquinas y procesos productivos de nuestras empresas, ya sean industriales o no, crean productos que pueden ofrecer a su vez servicios conectados. No debemos olvidar que digitalizar y conectar implica *hardware*, *software* (empotrado o no) y comunicaciones. Los ordenadores están dejando de ser en nuestra vida cotidiana esos

[1] Comisión Europea, "European Commission announces the Key Strategic Value Chains", 17/II/2019, https://s3platform.jrc.ec.europa.eu/-/european-commission-announces-the-key-strategic-value-chains?inheritRedirect=true.

elementos físicos visibles en nuestras casas y empresas para formar parte de objetos cotidianos que se convierten en inteligentes y que, a su vez, forman parte de sistemas que a su vez se conectan con otros, creando un mundo de sistemas de sistemas en donde los ordenadores siguen existiendo de forma transparente para sus usuarios. En definitiva, estamos hablando de ordenadores y redes que, aunque no los veamos físicamente como tales, no quiere decir que no existan, y, por tanto, hablamos de potenciales problemas de ciberseguridad causados por vulnerabilidades existentes en los equipos que puedan ser explotadas con fines no éticos.

Como resultado, los sistemas son cada vez más autónomos, pueden tomar sus propias decisiones e interactuar con el mundo físico a través de los sistemas ciberfísicos que podemos encontrar, por ejemplo, en las plantas industriales o en los vehículos conectados. Como ejemplo, la figura 1 muestra cómo los vehículos con sistemas de trasporte inteligentes y cooperativos se comunican entre sí y con las señales de tráfico y las infraestructuras viarias.

Figura 1. Ilustración de la interacción típica que existe dentro de una red C-ITS



Fuente: Cooperative Intelligent Transport System (C-ITS)[2]

Los retos que superar

La economía y la sociedad digital en las que vivimos se basan en la confianza en el buen funcionamiento de todos estos sistemas, que puede verse minada por

[2] Comisión Europea, DG Move, figura extraída del C-IT Platform. Final Report, enero de 2016, p. 52, https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.

ciberataques que exploten vulnerabilidades existentes. Por este motivo, la ciberseguridad adquiere una gran relevancia en todos los aspectos de nuestras vidas y nos permite hacer frente tanto a amenazas de confidencialidad, que pueden afectar a la privacidad, como a amenazas de integridad y disponibilidad de los sistemas, que pueden llegar a impactar en la seguridad física. De esta forma, la ciberseguridad se convierte en la guardiana de nuestra economía, sociedad e incluso de la salud de las actuales democracias[3], ayudando a preservar la confianza en todos estos sistemas.

La importancia de que los sistemas funcionen de una forma segura y resiliente implica trasladar la seguridad a todos los objetos, sistemas y sistemas de sistemas, aunque en este último caso nos podamos encontrar con la complejidad añadida de que la superficie de ataque puede aumentar a veces de forma impredecible. La ampliación obliga a garantizar la ciberseguridad durante el proceso completo de desarrollo de sistemas (*hardware*, *software*, conectados) y garantizar la ciberseguridad a lo largo de toda la cadena de suministro, con las consiguientes implicaciones.

Muchas de las vulnerabilidades utilizadas por los ciberatacantes explotan errores de *software* en funcionamiento, *software* malicioso como el desbordamiento de búfer (*buffer overflow*) o *software* que ha podido estar cumpliendo con su misión sin problemas durante años hasta que un ciberatacante decide convertir ese error en una vulnerabilidad que utilizar para un ataque. Esto puede ocurrir por la forma artesanal en la que se ha venido –y se sigue– desarrollando el *software* en muchas organizaciones, por la que se da prioridad a las funcionalidades que puede ofrecer un nuevo equipamiento sobre su seguridad. Lo que prima en los procesos de desarrollo de *software* es la rapidez para sacar nuevos productos al mercado cuanto antes, que sean atractivos en términos de rendimiento y facilidad de uso y, sobre todo, que reduzcan los costes de desarrollo tanto como sea posible, lo que tiene consecuencias en términos de calidad o seguridad del *software* desarrollado y entregado posteriormente.

Esta forma de desarrollar el *software* ha empezado a dar quebraderos de cabeza y problemas de distinta envergadura en función de la empresa o sector, Administración o Estado del que hablemos y podría ser el comienzo de una tormenta perfecta si no se adoptan medidas que presten a la ciberseguridad del *software* la atención que merece a lo largo de todo el ciclo de su desarrollo dentro de una empresa.

Las medidas que tomar

La cadena de valor formada por una gran organización compradora de *software* y su red de proveedores tiene que tomar medidas para mejorar la calidad del *software* desarrollado y reducir los costes y los tiempos de entrega. Con independencia de si se utilizan metodologías ágiles o no, la industria del *software* debe incorporar requisitos de ciberseguridad, utilizar arquitecturas y diseño seguros, utilizar los estándares aplicables y realizar las verificaciones y validaciones necesarias, incluidas las fases finales de puesta en producción y de fin de la vida del producto.

[3] BELFER Center Science and International Affairs, “The Cybersecurity Campaign Playbook”, mayo de 2018, http://www.iri.org/sites/default/files/european_campaign_playbook_-_web.pdf.

(cont.)

La industria del *software* debe superar retos que se han superado en otros sectores. Entre otros, y según Iker Martínez[4], el cambio constante de requisitos es una moneda común en la industria de *software*, algo que no ocurre en otros sectores. Sería impensable que se realizaran cambios constantes en el recorrido de una carretera o que se cambiaran los materiales de un puente a mitad de obra sin pensar cuál sería su efecto.

Igual ocurre con la arquitectura y diseño del *software*, que apenas se valoran. Es como si en la construcción de una central térmica no se tuvieran en cuenta las implicaciones del diseño y la arquitectura para su funcionamiento y seguridad o se tuvieran en cuenta tras la construcción para cumplimentar la documentación. La industria del *software* tampoco suele tener en cuenta la verificación y validación, salvo si se ha producido un error, para solucionarlo. Es como si se pusiera en marcha un poste de alta tensión cerca de una vivienda sin realizar todas las pruebas necesarias para garantizar su seguridad. A lo anterior hay que añadir lo que le cuesta a la industria del *software* automatizar los procesos de ingeniería, a diferencia de la industria manufacturera, que ha automatizado la detección de errores y ha eliminado los procesos manuales de la cadena de montaje para evitar fallos en los productos finales.

Como en todo, siempre hay honrosas excepciones, porque evidentemente no todos los procesos de desarrollo de *software* son iguales ni en todas las empresas ni en todos los sectores, y entre los que cuentan con procesos de desarrollo de *software* de calidad podemos hablar, por ejemplo, del sector bancario. Sin embargo, esto no es suficiente, y las medidas indicadas deberían extenderse a todos los productos y sectores de una u otra forma.

En este sentido, las industrias no de *software* y las ingenierías se encuentran con mayores dificultades para la incorporación de procesos de desarrollo de *software* seguro al no contar, en general, con los perfiles técnicos apropiados de desarrollo de *software*. Las dificultades obedecen a la falta de profesionales de ciberseguridad, como ingenieros o arquitectos de ciberseguridad, y la escasa formación en ciberseguridad de gran parte de los ingenieros de *software* y de otras ingenierías que finalmente acaban desarrollando *software* en las empresas. No deja de resultar curioso que en muchas empresas se piense que el *software* puede realizarlo cualquier persona y que basta con que haya hecho un curso de programación o bien que sea autodidacta y le guste programar. No tienen en cuenta el riesgo de ciberseguridad que corren cuando conectan el *software* de sus productos a Internet o cuando lo integran en alguna cadena de valor, algo que no sucede en ningún otro ámbito.

Del mismo modo, las empresas e industrias que subcontratan los desarrollos de *software* a otra empresa o aquellas que integran diferentes productos de distintos proveedores en su cadena de suministro tienen que requerir a sus proveedores las mismas exigencias de ciberseguridad que les empiezan a solicitar a ellas sus clientes y usuarios. En este sentido, es fundamental que esas empresas fijen en el modelo de

[4] Iker Martínez de Soria (2016), "Oportunidades en la industria del software", Blog Tecnalia, 24/V/2016, http://blogs.tecnalia.com/inspiring-blog/2016/05/24/industria-del-software/.

(cont.)

gestión y de relación que tengan establecido con sus proveedores los indicadores de control de la ciberseguridad necesarios. Tampoco deben olvidar que los subcontratados en tareas de desarrollo pueden convertirse en amenazas internas[5] o que, si los proveedores no se preocupan por la ciberseguridad, pueden permitir el acceso a datos de las empresas[6] o facilitar que se aproveche la vulnerabilidad del eslabón más débil de la cadena para realizar ciberataques al resto de ella.

Las empresas e industrias deben incorporar la ciberseguridad desde el diseño inicial y tenerla en cuenta para todo el ciclo de vida del producto, proceso o servicio, así como la ciberseguridad por defecto en productos y servicios, ofreciendo una primera configuración lo más segura posible que permita reducir la carga del usuario en la configuración. Esto no es tan fácil de realizar, porque el mercado no valora suficientemente las ventajas de la ciberseguridad y penaliza el mayor coste de los productos con mejores garantías de ciberseguridad, por lo que el gasto difícilmente se podrá repercutir al cliente, penalizando los resultados de las empresas. En la práctica, sólo asumen el coste de la ciberseguridad aquellas empresas o industrias que se preocupan por reducir el riesgo de una parada de producción o de un accidente o las que están obligadas por alguna regulación.

También debemos considerar que estamos acostumbrados a que tanto los fabricantes de *hardware* como de *software* no tengan responsabilidades si algo va mal, ya que las pérdidas las asumen los usuarios. En el contexto actual, y teniendo en cuenta que algunos productos pueden estar sujetos a leyes de responsabilidad civil, debemos empezar a pensar qué va a pasar con sus productos conectados si algo va mal por el *software* que llevan. A esto debemos añadir las dificultades en determinados casos para asegurar que un determinado fallo ha podido ser debido a un ciberataque que ha explotado una vulnerabilidad del producto.

Bruce Schneier, en su conocido libro *Haz clic aquí para matarlos a todos. Un manual de supervivencia*, destaca tres ámbitos en los que las políticas deben actuar para fomentar un comportamiento seguro:

- *Ex ante*, estableciendo reglas para evitar que sucedan cosas malas. Comprende regulaciones sobre productos y categorías de productos, licencias de profesionales y productos y requisitos de prueba y certificación que establezcan mejores prácticas en la industria y beneficios por hacer las cosas bien.

- *Ex post*, con reglas que castigan el mal comportamiento una vez que algo malo ha ocurrido. Incluye multas por falta de seguridad y atribuciones de responsabilidades cuando las cosas salen mal.

[5] Agustín Marco (2019), "Naturgy sufre el chantaje de un 'hacker' que robó información ultraconfidencial", *El Confidencial*, 18/VII/2019, https://www.elconfidencial.com/empresas/2019-07-18/naturgy-chantaje-robo-informacion-confidencial-ciberataque_2130979/.

[6] "Naturgy prescinde de Capgemini como proveedor de ciberseguridad", *Computing*, 19/VII/2019, https://www.computing.es/seguridad/noticias/1113328002501/naturgy-prescinde-de-capgemini-proveedor-de-ciberseguridad.1.html.

- Divulgación mediante leyes de etiquetado de productos y otras modalidades.

Por su parte, la UE ha comenzado a actuar en diferentes frentes, por ejemplo aumentando los costes de la inseguridad, como es el caso de las penalizaciones por incumplir el Reglamento General de Protección de Datos, o creando incentivos como el reglamento europeo para la certificación de productos y servicios TIC (Cybersecurity Act). En este último se menciona, en relación con las cadenas de suministro, que los fabricantes, proveedores de productos, servicios o procesos de TIC deben aportar las actualizaciones necesarias y recuperar, retirar o reciclar los productos, servicios o procesos de TIC que no cumplan las normas de ciberseguridad, mientras que los importadores y distribuidores deben asegurarse de que los productos, servicios y procesos de TIC que introduzcan en el mercado cumplan los requisitos aplicables y no supongan un riesgo para los consumidores europeos. El cumplimiento de las regulaciones y certificaciones propiciadas por la UE obligará a corto plazo a las empresas e industrias con productos o procesos más críticos para la economía, pero deben empezar a darse pasos para realizar cambios de cara al largo plazo, en el que la formación y la capacitación serán piezas claves para fomentar una cultura de la ciberseguridad desde el diseño y por defecto.

Conclusiones

La ciberseguridad es compleja y multidimensional. Tiene una dimensión tecnológica, ya que para desarrollar soluciones de ciberseguridad se utilizan tecnologías como la criptografía, la inteligencia artificial, la cadena de bloques o registros distribuidos, entre otras. Abarca no sólo *software*; también *hardware*, comunicaciones y sistemas de sistemas con complejas cadenas de valor. La ciberseguridad tiene campos de aplicación en todos los sectores en los que podamos pensar, desde la energía a la salud, pasando por los servicios públicos. Por otro lado, los ciberatacantes pueden estar en cualquier parte del mundo y cualquier avance tecnológico es rápidamente utilizado por ellos para perpetrar ataques más sofisticados. La ciberseguridad tiene dimensiones técnicas, económicas, sociológicas, educativas, de defensa y políticas que deben contemplarse de forma holística e integrada para lograr las masas críticas y los niveles de excelencia necesarios para reforzar la cadena de valor de la ciberseguridad tanto para los proveedores como para los clientes y poder mantener la confianza en la digitalización.

Debe actuarse en varios frentes. En el frente industrial se debe:

- Crear una cultura de hacer las cosas bien desde el principio y poder solucionar los problemas rápidamente cuando surjan. Esto implica crear una cultura de la ciberseguridad desde el diseño y por defecto que no sólo sea aplicable a los productos y servicios, sino también a las nuevas tecnologías.

- Promover la creación de estándares y certificaciones que faciliten a las empresas la prevención, detección y respuesta a los ataques cibernéticos y creen confianza sobre el nivel de seguridad de los productos, servicios y procesos de TIC. Una certificación simplifica la complejidad que hay detrás de un producto o sistema al usuario final y le tranquiliza respecto a su utilización.

- Promover la utilización en todos los productos de la denominado “raíz de confianza”, de tal forma que se parta de componentes base, *hardware* o *software* certificados y a partir de ellos se construyan el resto de los sistemas como capas sucesivas.

- Promover la asignación de responsabilidades ligadas al mal funcionamiento de dispositivos conectados para que, si las cosas van mal, las consecuencias no las tenga que asumir el usuario.

- Promover un etiquetado de ciberseguridad útil y sencillo para los usuarios de los productos, tal y como existe en otros sectores, que permita comparar características de seguridad entre productos, durante cuánto tiempo mantendrá esas características el fabricante y cuándo pasarán a ser por cuenta y riesgo del usuario.

- Promover que la I+D y la ciberseguridad deben ir de la mano con un equilibrio entre beneficiarse de las nuevas tecnologías y al mismo tiempo construirlas seguras.

En el ámbito de la educación y la formación, se deben promover políticas educativas específicas y alineadas con las políticas industriales:

- Aumentar la educación pública en ciberseguridad enseñando a vivir en el mundo digital lo mismo que en el mundo real y permitiendo a todos los ciudadanos un conocimiento básico que les permita gestionar la ciberseguridad sin necesidad de ser expertos.

- Definir estándares profesionales en ciberseguridad, ya que no hay ningún sistema para certificar o licenciar a los diseñadores de *software*, arquitectos de seguridad, ingenieros informáticos o programadores. Podría plantearse que un diseño de *software* lleve la firma de un profesional cualificado, lo mismo que se exige la firma de un arquitecto colegiado en los diseños de obra.

- Capacitar a los ingenieros de diferentes especialidades que posteriormente estarán implicados en tareas de desarrollo en el diseño y desarrollo seguro de *software*.

- Concienciar a las empresas de la importancia creciente del *software* para sus productos y de que el proceso de desarrollo de *software* debe profesionalizarse.

El camino va a ser largo y complicado, pero el objetivo es conseguir que nuestra sociedad y nuestra economía sean resilientes frente a los ciberataques. Para reforzar su “sistema inmunológico”, se precisa adoptar medidas como las indicadas para contar con una industria de la ciberseguridad más fuerte y competitiva, que permita aumentar los niveles de protección y de respuesta ante incidentes de los usuarios, ya sea ciudadanos, empresas o Estados, con soluciones apropiadas de ciberseguridad, logrando el liderazgo en áreas claves de la ciberseguridad que permita ampliar la cuota de mercado internacional.