La ciberseguridad: un asunto de todos, un asunto de Europa.

Estamos inmersos en un proceso de transformación digital a nivel mundial en el que tanto las administraciones públicas como el sector privado y los propios ciudadanos están jugando un papel fundamental, dado que la tecnología ya está presente en todos los ámbitos de nuestras vidas y en la forma en la que nos relacionamos.

ALBERTO HERNÁNDEZ
Director General del Instituto Nacional de Ciberseguridad (INCIBE) hasta noviembre de 2019.

La ciberseguridad se ha convertido en una variable esencial y prioritaria para que este proceso de transformación no genere en las organizaciones y en la propia sociedad efectos negativos que desvirtúen los beneficios esperados.

En los últimos años hemos experimentado un incremento significativo en el número e impacto de los ciberataques a nivel internacional. En el caso de España, desde el Centro de Respuesta ante Incidentes (INCIBE-CERT) del Instituto Nacional de Ciberseguridad (INCIBE), gestionamos sólo en el año 2018 más de 111.000 incidentes de ciberseguridad que afectaron a ciudadanos y empresas. En el año 2014 esta cifra fue de 18.000, lo que pone de manifiesto la importancia y gravedad del problema dado el más que significativo incremento en el número de ciberataques que se está produciendo año a año. A esto hay que añadir lo difícil de cuantificar cuántos incidentes dejamos de detectar, ya que su sofisticación aumenta día a día y su impacto ya no es tan evidente a corto plazo. Las nuevas formas de malware buscan infectar por el mayor tiempo posible los sistemas y las redes informáticas intentando pasar desapercibidos el mayor tiempo posible, tiempo durante el cual roban información muy valiosa para la organización afectada.

¿Qué debemos hacer por tanto para protegernos ante esta nueva situación? Desde INCIBE trabajamos en numerosas líneas de acción orientadas no sólo a la detección, análisis, notificación y respuesta ante ciberataques, sino también en el ámbito de la prevención. La prevención es sin duda el elemento

“El ciberespacio es global, no tiene fronteras, no pertenece a ningún Estado en particular, presenta asimetría, es potencialmente vulnerable, las acciones que ocurren en él tienen un impacto en tan sólo unos milisegundos y su ciberseguridad es entendida de forma diferente en muchos países. Y esto último es de capital importancia para poder llegar a desarrollar iniciativas internacionales que persigan de manera efectiva el ciberdelito.”

fundamental a tener en cuenta para garantizar que si bien seguiremos recibiendo ciberataques en el futuro, su impacto sea el mínimo posible. En el ámbito de la concienciación, desde INCIBE hemos venido lanzando numerosas iniciativas en estos últimos años para elevar el nivel de conocimiento y comprensión de los riesgos de ciberseguridad en el uso de las tecnologías digitales y las normas básicas a adoptar para tener un nivel mínimo de protección. No obstante, si analizamos los problemas más comunes que están afectando a día de hoy a los ciudadanos y empresas nos damos cuenta de que hay mucho por hacer.

Es importante además recordar que el ciberespacio es global, no tiene fronteras, no pertenece a ningún Estado en particular, presenta asimetría, es potencialmente vulnerable, las acciones que ocurren en él tienen un impacto en tan sólo unos milisegundos y su ciberseguridad es entendida de forma diferente en muchos países. Y esto último es de capital importancia para poder llegar a desarrollar iniciativas internacionales que persigan de manera efectiva el ciberdelito.

Un ejemplo que nos ayudará a entender las diferentes formas en las que los países perciben la ciberseguridad y que puede dificultar la persecución del ciberdelito es la conservación de los datos de navegación cuando nos conectamos a Internet. En España y en Europa contamos con una ley de conservación de datos por la que los operadores de telecomunicaciones están obligados a conservar los datos de navegación de nuestras conexiones a Internet durante un cierto tiempo. De esta forma, ante un delito y bajo autorización judicial, el operador debe proporcionar dichos datos de navegación a las fuerzas y cuerpos de seguridad para que puedan avanzar en la investigación y puedan identificar el origen del delito. Pero en otros países del mundo, bien por razones políticas, sociales e incluso históricas o una mezcla de todas ellas, se está entendiendo esta conservación de datos como una posible vulneración de derechos fundamentales como es el de la privacidad. Si tenemos en cuenta que la gran mayoría de ciberataques que están afectando a España se originan a miles de kilómetros de distancia y antes de llegar a nuestro país han pasado a través de sistemas y redes de otros países, es fundamental para la identificación del origen del ataque que se disponga del histórico de datos en todos y cada uno de los países.

En la Unión Europea la ciberseguridad se ha convertido en una prioridad estratégica de primer nivel, lo que demuestra la propia Estrategia Europea de Ciberseguridad o el conjunto de iniciativas que se están desarrollando para fortalecer la Unión Europea a todos los niveles: regulatorio, social y de competitividad de la industria de ciberseguridad. Prueba de ello es que en 2018 se ha completado la transposición en el ordenamiento jurídico de cada uno de los Estados Miembro de la Directiva NIS (Network and Information Security) así como la adecuación al Reglamento Europeo de Protección de Datos. Esto ha supuesto un enorme avance hacia la creación de un espacio europeo común en ciberseguridad, la protección de ciudadanos y empresas, la garantía de derechos democráticos, así como la mejora de los esquemas de gobernanza y coordinación en situaciones de ataques cibernéticos que afecten al espacio europeo.

En la Unión Europea todos los Estados Miembro estamos trabajando y colaborando de forma muy estrecha, dado que la ciberseguridad no sólo supone un reto a la seguridad nacional de cada país sino también un reto a la propia seguridad internacional.

Esta colaboración se sustenta básicamente en dos pilares:

1. La mejora y reforzamiento de los mecanismos de intercambio de información de ciberseguridad entre todos los países, especialmente aquella información orientada a la alerta temprana, de modo que se puedan establecer medidas de carácter preventivo y reactivo que mitiguen el impacto de un posible ciberataque. La mejora también de la colaboración en la respuesta ante una crisis nacional o europea motivada por un ciberataque.

2. El desarrollo de la industria europea de ciberseguridad, ya que este nuevo sector puede suponer una gran oportunidad para la creación de nuevas empresas o la internacionalización de las ya existentes, creando en definitiva cientos de miles de puestos de trabajo en los próximos años.

De acuerdo con un estudio de ECSO (European Cybersecurity Organization), a día de hoy de las 500 mejores empresas de ciberseguridad del mundo sólo 14 son europeas teniendo una cuota total del mercado del 23%. Si tenemos en cuenta que la cuota de mercado de las empresas de EEUU supone ya el 46% del total y que se espera que en 2023 la cuota de mercado que tengan las empresas de los países asiáticos supere el 30%, en 3 o 4 años el 70-80% del mercado global de la ciberseguridad estaría copado por empresas asiáticas y estadounidenses. Es por ello que desde la Unión Europea debemos trabajar de forma comprometida en apoyar nuestro desarrollo industrial.

Una de las herramientas necesarias para mantener un mínimo de ciberseguridad en la Unión Europea, pero que también condiciona e impulsa el desarrollo industrial, es la definición de un esquema de certificación de productos, sistemas y servicios. Recientemente ha sido publicado el nuevo reglamento de la agencia europea ENISA (European Union Agency for Cybersecurity) en el que es designada para liderar el desarrollo de un esquema de certificación de productos, sistemas y servicios de ciberseguridad en el ámbito de la Unión Europea.

Una de las acciones prioritarias para tener un espacio digital ciberseguro es garantizar que la tecnología digital y los servicios que se basan en ella cumplan unos mínimos de ciberseguridad. Estos mínimos no deben no obstante, limitar o restringir el desarrollo de la industria sino, garantizando un nivel de ciberseguridad adecuado, la industria pueda ser competitiva en este mercado global.

En el caso de España, en el que el sector de la ciberseguridad está compuesto fundamentalmente por pequeñas y medianas empresas salvo algunas pocas grandes empresas, el esquema de certificación que se desarrolle es de vital importancia para su supervivencia. Desde el punto de vista de INCIBE, debemos apostar por el desarrollo de un esquema que garantice adecuados niveles de ciberseguridad de la tecnología pero que no supongan una barrera en cuanto a su coste, pues de otra forma no podría ser asumido por nuestras empresas.

Además de esta colaboración necesaria entre Estados Miembro en el seno de la Unión Europea, se está produciendo una competición entre todos los países para que el conjunto de iniciativas que se lancen beneficien de forma directa a su industria nacional. En este sentido, la Unión Europea prevé aprobar este mismo año la creación de un Centro Europeo de Competencia en Ciberseguridad Industrial, Tecnología e Investigación así como una Red de Centros Nacionales de Coordinación en dichas materias. Todo ello con el objetivo de agilizar, de manera coordinada entre estos organismos, las actividades e inversiones que faciliten la I+D+i y el desarrollo industrial en la Unión Europea. En este momento son varios los países, incluido España, que están apoyando está iniciativa.

Sin lugar a dudas, disponer de una industria competitiva en ciberseguridad permitirá además incrementar la confianza en la tecnología y las redes de comunicación de los ciudadanos europeos.

En definitiva, la ciberseguridad supone un reto a nuestra seguridad nacional pero que requiere del esfuerzo y compromiso no sólo de los organismos públicos que trabajamos en ella, sino de todo el sector privado y de los propios ciudadanos que utilizan la tecnología. Además, la ciberseguridad es una oportunidad para el desarrollo económico de Europa que debemos aprovechar. ✱