La gestión regulada de incidentes de ciberseguridad, un nuevo paso

Pocos discuten ya que la seguridad de la información está adquiriendo una importancia creciente para nuestra economía y nuestra sociedad y que dicha seguridad es imprescindible para crear un mercado único europeo electrónico, altamente competitivo y al mismo nivel o superior que otros mercados que todos tenemos en mente. Tal hecho está provocando que los Estados aborden reformas normativas en donde este hecho queda patente. Un buen ejemplo lo tenemos en la nueva Ley de Telecomunicaciones y en sus efectos sobre la LSSI-CE, que tocan de lleno a la gestión de incidentes de ciberseguridad y a los agentes involucrados.

Alonso Hurtado Bueno

Si atendemos a los datos hechos públicos por parte de la Comisión Europea, el 57 % de los participantes en las encuestas realizadas por la Comisión ha sufrido a lo largo del año 2012 incidentes de seguridad que han tenido graves consecuencias en sus actividades. La falta de seguridad, pues, puede llegar a comprometer servicios vitales que dependen de la integridad de las redes y los sistemas de información, interrumpiendo las actividades de las empresas, generando cuantiosas pérdidas financieras para la economía o poniendo en riesgo la propia seguridad nacional de los Estados y, cómo no, del resto de países con los que estos se relacionen habitualmente.

Es precisamente esta característica innata del medio, la globalidad y su carácter transfronterizo, lo que hace que la resiliencia y la estabilidad de las redes y cualquier tipo de sistema de información revistan suma importancia para lograr la consecución del mercado único digital y el buen funcionamiento del mercado interior de la Unión Europea.

La mayor probabilidad o frecuencia de los incidentes y la incapacidad de ofrecer protección suficiente llevan aparejada, indudablemente, una pérdida de confianza de los ciudadanos en los servicios electrónicos, retrasando la normal evolución de un mercado que se postula como el principal en el que se desarrollará la actividad económica habitual en los próximos años.

Hasta el momento, la situación en la mayoría de los actores implicados en la Unión Europea era, (y en gran parte lo sigue siendo), un reflejo del planteamiento meramente voluntario, en el que eran los propios actores, ya fueran empresas privadas u organismos públicos, los que voluntariamente decidían si implantaban medidas de seguridad adecuadas para proteger tanto su información, como su infraestructura, no existiendo apenas reglas, legalmente vinculantes, que establecieran cuál era el nivel de protección suficiente frente a incidentes y riesgos relacionados con la seguridad de la información, ni los medios especializados para comunicar los incidentes de ciberseguridad detectados.

Nueva Ley de Telecomunicaciones y modificaciones en la LSSI-CE

En este sentido, desde hace escasos 4 años, el mundo de Internet en general y de la ciberseguridad en particular ha iniciado un camino de no retorno en lo que a su regulación normativa se refiere. Desde que en el año 2010 se aprobara el Real Decreto 3/2007 por el que se aprueba el Esquema Nacional de Seguridad, hemos asistido a una incesante aprobación de textos normativos en los que, o bien íntegramente se abordaban cuestiones concretas y particulares relacionadas con la ciberseguridad, o bien se introducían modificaciones en normas ya vigentes en nuestro ordenamiento jurídico, que actualizan o introducen obligaciones adicionales en materia de Ciberseguridad.

Sin ánimo de realizar una relación completa de todas y cada una de las normas de aprobación relativamente reciente que tratan directamente las obligaciones en materia de ciberseguridad, cabe destacar la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su Reglamento de desarrollo, la Ley 5/2014 de Seguridad Privada, la Estrategia Nacional de Ciberseguridad aprobada a finales del año 2013 o la reciente Ley 9/2014 de Telecomunicaciones, encargada de introducir en la Ley 34/2002 varias modificaciones directamente relacionadas con la ciberseguridad.

Concretamente y por tratarse de la última norma aprobada que introduce regulación específica en materia de ciberseguridad, debe tenerse en consideración la reciente Ley 9/2014, de 9 de mayo, de Telecomunicaciones, que en su Disposición Adicional Segunda, apartados quince y dieciséis, se modifica la Disposición Adicional Octava y Novena de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante LSSI-CE)

Concretamente, la citada modificación normativa se centra en dos ejes fundamentales y que desde nuestro punto de vista venían siendo extraordinariamente necesarios en nuestro ordenamiento jurídico. Estos son:

En primer lugar, se establece la **obligación de colaboración, por parte de los agentes del mercado implicados, con las autoridades competentes** imponiéndose la obligación sobre los diferentes actores implicados de facilitar toda la información, datos o evidencias que faciliten o en su caso permitan la persecución de actividades ilícitas en el ciberespacio.

Concretamente, los agentes implicados que deberán colaborar con los CERT, o Equipos de Respuesta a Incidentes de Seguridad de la Información a los que hace referencia expresa la citada norma, son los siguientes:

a) Entidades de Registro de Nombres de Dominio establecidos en España.

b) Los Equipos de Respuesta de Incidentes de Seguridad Públicos.

c) Los Prestadores de Servicios de la Sociedad de la Información establecidos en España.

Concretamente la modificación introducida es clara en determinar lo que se va a

La modificación introducida en la Disposición Adicional Novena de la LSSI-CE plantea jurídicamente algunas dudas, en tanto supone la imposición legal de bloqueo semiautomático de cualquier servicio o infraestructura que pueda suponer un riesgo para la red, sin que para ello sea necesario contar con autorización previa de la autoridad competente.

convertir en eje fundamental para lograr dotar al ciberespacio, al menos dentro de las fronteras de España y de la Unión Europea, de un mayor grado de coordinación y de seguridad. Lejos de pensar que se trata de la imposición de medidas de seguridad específicas, se centra en determinar **la obligación de los tres principales actores del ciberespacio** y sobre los que se sustentan tanto las infraestructuras de Telecomunicaciones como los servicios que corren sobre las mismas, **de compartir información respecto a los incidentes de Ciberseguridad que se hayan podido producir en sus plataformas, servicios o infraestructuras** (identificación de origen, destino, riesgos asociados y efectos producidos con las autoridades competentes)

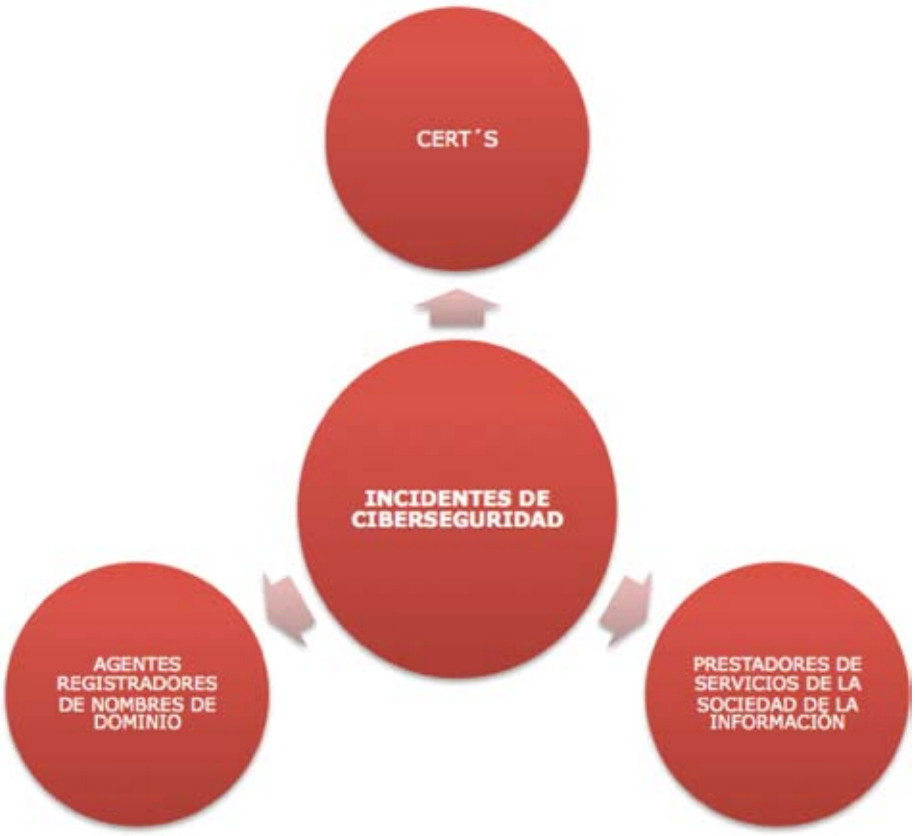
En segundo lugar se introduce una nueva modificación normativa en la Disposición Adicional Novena de la LSSI-CE, siendo ésta la que desde un punto de vista jurídico introduce mayores dudas, en tanto supone la **imposición legal de bloqueo semiautomático de cualquier servicio o infraestructura que pueda suponer un riesgo para la red, sin que para ello sea necesario contar con autorización previa de la autoridad competente**.

El supuesto de hecho es relativamente sencillo, además de habitual. Una plataforma web, operada bajo un nombre de dominio ".es" y alojada en un proveedor de servicios de alojamiento (ISP) dispone de software malicioso (ya sea introducido voluntariamente o no) que puede estar permitiendo que dicha plataforma sea utilizada como tal para llevar a cabo acciones delictivas en la red y por tanto, suponiendo un riesgo para el resto de actores.

En este caso, el proveedor de alojamiento, así como el agente registrador del nombre de dominio, una vez detectado que el sitio web en cuestión puede estar siendo origen de algún incidente de ciberseguridad, deben, de oficio, y sin necesidad de obtener ningún tipo de autorización por parte de la autoridad competente, paralizar o poner en "cuarentena" la plataforma *online* en cuestión que se encuentre afectada por el incidente de seguridad, garantizando así que el riesgo para el ciberespacio es anulado en su origen.

Desconexión sin autorización previa

Como se indica, la normativa ampara expresamente que esta acción de desconexión puede ser realizada sin ningún tipo de autorización previa por parte de la autoridad competente, sino que basta únicamente con que el Prestador de Servicios o Agente Registrador de dominios preavise al titular de la plataforma en línea que está viéndose afectada por un incidente de ciberseguridad.



Las modificaciones normativas consagran la colaboración de CERTs, Agentes Registradores y Prestadores en la gestión de incidentes.

Desde luego, teniendo en cuenta la facilidad de propagación de la mayoría de ataques de ciberseguridad y el efecto de escalado y replicación que una plataforma *online* infectada puede suponer, no sólo para el propio prestador de servicios de la sociedad de la información ubicado en España, sino para cualquier usuario o prestador que opere en Internet, hacen que al menos desde el punto de vista práctico y sobre todo, desde el objetivo último de lograr minimizar los riesgos para el ciberespacio y el resto de actores que operan el mismo, nos haga plantearnos si existe, teniendo en cuenta la rapidez con la que es necesario actuar en estos casos, alguna alternativa viable a la introducida por la normativa comentada.

A modo de conclusión, cabe afirmar que los Estados van tomando consciencia de la importancia que va a jugar (y que ya está jugando en algunos ámbitos) el ciberespacio y la seguridad del mismo en el desarrollo económico y social de nuestras sociedades, por lo que comenzamos a ver cambios normativos encaminados a dotar de las medidas de seguridad, tanto de carácter organizativo o carácter operacional, como de protección, a los diferentes agentes implicados.

A pesar de ello, desde nuestro punto de vista, debe apostarse de forma clara y lo antes posible, por la aprobación de una normativa común [1], si no de nivel global (dada la complejidad para lograr una empresa de ese tipo), sí de carácter internacional a nivel comunitario, que defina una serie de reglas y obligaciones que todos los agentes del mercado implicados en la ciberseguridad deban cumplir, de tal forma que las respuestas a los incidentes de ciberseguridad sean realizados de forma uniforme y absolutamente coordinada, dando así soluciones globales a los retos globales que el ciberespacio nos plantea a diario. ■

[1] Para más información Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes de la información en la Unión Europea. Disponible para su descarga desde el siguiente link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:ES:PDF (PDF)

Alonso Hurtado Bueno
Socio – Information Technology
ECIJA
alhurtado@ecija.com