3 La Directiva de Seguridad de las Redes y de la Información (NIS)

Regulación para la ciberseguridad

Como continuación de la noticia anterior donde hablamos de los aspectos a considerar por lo negocios online, en este segundo artículo trataremos cómo la Unión Europea y por extensión sus Estados Miembros se enfrentan a una serie de retos que resaltamos a continuación.

En 2013, la Comisión presentó una propuesta de Directiva relativa a las medidas para garantizar un elevado nivel común de las redes y la información de seguridad en toda la Unión. Dos años más tarde, el Parlamento y el Consejo acordaron en el texto de la Directiva de red y seguridad de la información (NIS). Se espera que, en los próximos meses, el Parlamento y el Consejo de la Unión Europea aprueben formalmente la Directiva, tras lo cual se publicará en el Boletín Oficial de la Unión Europea. Los Estados Miembros tendrán veintiún meses para transponer la Directiva NIS a una Ley nacional y seis meses adicionales para identificar los operadores de servicios esenciales**.**

Retos de la directiva NIS

Muy probablemente, la transposición por parte de cada Estado Miembro derivará en planes de ciberseguridad distintos donde se exijan medidas de ciberseguridad diferentes en varios países de la Unión Europea. A día de hoy existen diferentes grados de madurez de ciberseguridad entre los Estados Miembros, y, como consecuencia, la transposición nacional podría llevar a una mayor fragmentación en distintas definiciones del plan de ciberseguridad en cada país. Es probable que algunos países sean más estrictos en la interpretación que otros, como se ha evidenciado con la Directiva Europea de Protección de Datos (95/46/EC). Esta diversidad en la interpretación podría producir un desnivel en la protección de los consumidores y empresas en función de las exigencias impuestas en cada Estado miembro, así como suponer una barrera para compañías que deseen operar en distintos países europeos de forma simultánea. Por lo tanto, sería importante que la propuesta de NIS sea única y global en la Unión Europea y que existan unos requisitos idénticos y un nivel mínimo de exigencia en todos los países.

Las pequeñas y medianas empresas, al no estar obligadas a cumplir con la Directiva, se convertirán en el punto más débil de la cadena. Tampoco se espera que las empresas fabricantes de software o hardware se vean afectadas por la Directiva, lo que se antoja sorprendente ya que parecería que deberían ser las primeras en el cumplimiento de los requisitos básicos de seguridad y privacidad en cuanto al diseño de sus productos y servicios. Todas estas empresas, al no estar sujetas al cumplimiento de un mínimo de medidas de seguridad o a la notificación de incidentes, pueden potencialmente crear un escenario que las haga objetivo del cibercrimen. No olvidemos que las pequeñas y medianas empresas suman el mayor porcentaje de empresas que utilizan infraestructuras de seguridad de redes e información. La Unión Europea quizás debería imponer un mínimo de requisitos de obligado cumplimiento e incluso algún tipo de certificación voluntaria que permitiera varios niveles de madurez en la ciberseguridad.

Ciertos retos económicos tendrán que valorarse en función del grado de madurez de cada Estado Miembro, pues ya existen algunos países con planes de ciberseguridad, o incluso varios CSIRTs nacionales. También sería importante que se dotara a ENISA de los suficientes fondos para poder coordinar a los distintos CSIRTs nacionales.

Actualmente se desconoce cuáles serán los poderes específicos que tendrá la autoridad nacional competente (NCA) y el CSIRT nacional. Tampoco existe ningún tipo de guía sobre el solapamiento en las obligaciones de notificación de las distintas regulaciones como NIS y el futuro Reglamento General de Protección de Datos – GDPR, acrónimo del inglés General Data Protection Regulation –. Del mismo modo,

no se ha tenido en cuenta la posibilidad de que algunos operadores críticos estén sujetos a la notificación simultánea a distintos Reguladores nacionales e internacionales. En el caso de un banco español, por ejemplo, una fuga de datos personales es un incidente significativo se tendría que notificarse simultáneamente al Regulador nacional de protección de datos, al Regulador competente en infraestructura crítica, al Ministerio del Interior y al Banco Central Europeo. Todos estos retos ponen en evidencia la gran cantidad de Reguladores que pueden estar exigiendo las mismas responsabilidades, creando solapamientos regulatorios y, por lo tanto, añadiendo mayor complejidad y costes para las empresas y gobiernos. Un mecanismo único de notificación al estilo "one-stop-shop" permitiría mejorar la eficacia en las notificaciones, así como la reducción del coste y la complejidad del mismo.

También supone un reto identificar la forma más efectiva de notificación de incidentes entre entidades y los estándares que se han de utilizar. Establecer los mismos requisitos en todos los Estados Miembros evitaría distintas implementaciones y haría más efectiva la compartición de los incidentes con Entidades públicas y privadas. Igualmente, sería deseable que se pudiera contemplar una vía legal para poder compartir incidentes que contengan datos personales como la dirección IP de ordenadores infectados con malware que estuvieran participando en campañas de phishing a Entidades donde se haya cometido algún tipo de delito informático. De esta forma, las entidades afectadas podrían ser aún más proactivas y lograr una reducción significativa en los ciberataques, gracias a una más efectiva colaboración entre empresas públicas y privadas.

Aunque las medidas técnicas y organizativas impuestas a las empresas afectadas por la Directiva NIS inicialmente no requieren que un producto o servicio sea diseñado, desarrollado o fabricado de una forma particular, algunos países podrían tener la tentación de imponer un registro, homologación o proceso de certificación para productos y servicios. Si el objetivo de dicha imposición fuera el fomentar un mínimo grado de madurez en las empresas, sería imprescindible que todos los Estados Miembros llegaran a un acuerdo común para evitar la fragmentación. Posiblemente, una buena opción sería la creación de certificaciones optativas pero incentivadas, con distintos niveles de madurez e internacionalmente reconocidas como los estándares del European Telecommunications Standards Institute (ETSI) o IEEE-SA.

Conclusión

Las Autoridades competentes designadas en la transposición de la Directiva NIS podrán investigar casos de incumplimiento y sancionar si es necesario. Por lo tanto, tendrán el poder de realizar evaluaciones del nivel de ciberseguridad y exigir las medidas necesarias en los sistemas de información de las empresas. También podrán exigir auditorías de ciberseguridad a realizar por terceros. A falta de tener más información, existen dudas acerca de cuáles van a ser las exigencias respecto a las medidas de seguridad mínimas, si se basarán en estándares o auditorías internacionalmente reconocidas como ISO 27001, NIST o SSAE16 o si, por lo contrario, asistiremos a la creación de nuevos estándares. Tampoco se conoce si estos estándares y auditorías serán comunes en toda la Unión Europea o si cada país adoptara los suyos propios, creando una mayor fragmentación.

Aunque sin duda la Directiva NIS es un gran paso para la mejora de la ciberseguridad en Europa, aún tendremos que esperar a valorar como la Comisión Europea junto con ENISA resuelven estos retos mediante la promulgación de leyes y guías, las cuales se espera que especifiquen un mayor detalle respecto a la implementación de los planes estratégicos de cooperación o los estándares y especificaciones que podrán utilizarse para NIS.

AVISO LEGAL

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos, opiniones o estimaciones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

Las estimaciones que este documento puede contener han sido realizadas conforme a metodologías generalmente aceptadas y deben tomarse como tales, es decir, como previsiones o proyecciones. La evolución histórica de las variables económicas (positiva o negativa) no garantiza una evolución equivalente en el futuro.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

Especialmente en lo que se refiere a la inversión en activos financieros que pudieran estar relacionados con las variables económicas que este documento puede desarrollar, los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

Este informe ha sido elaborado por la unidad de Regulación Digital:

Economista Jefe de Regulación Digital
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Con la colaboración de:

Francisco Borja Larrumbide Martínes
fborja.larrumbide@bbva.com

Alfonso Arellano
alfonso.arellano.espinar@bbva.com

BBVA Research

Economista Jefe Grupo BBVA
Jorge Sicilia Serrano

Área de Economías Desarrolladas
Rafael Doménech
r.domenech@bbva.com

España
Miguel Cardoso
miguel.cardoso@bbva.com

Europa
Miguel Jiménez
mjimenezg@bbva.com

Estados Unidos
Nathaniel Karp
Nathaniel.Karp@bbva.com

Área de Economías Emergentes

Análisis Transversal de Economías Emergentes
Álvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

México
Carlos Serrano
carlos.serranoh@bbva.com

Turquía
Álvaro Ortiz
alvaro.ortiz@bbva.com

Coordinación LATAM
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Perú
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

Área de Sistemas Financieros y Regulación
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Sistemas Financieros
Ana Rubio
arubiog@bbva.com

Inclusión Financiera
David Tuesta
david.tuesta@bbva.com

Regulación y Políticas Públicas
María Abascal
maria.abascal@bbva.com

Regulación Digital
Álvaro Martín
alvaro.martin@bbva.com

Áreas Globales

Escenarios Económicos
Julián Cubero
juan.cubero@bbva.com

Escenarios Financieros
Sonsoles Castillo
s.castillo@bbva.com

Innovación y Procesos
Oscar de las Peñas
oscar.delaspenas@bbva.com

Interesados dirigirse a:

BBVA Research
Calle Azul, 4
Edificio de la Vela - 4ª y 5ª plantas
28050 Madrid (España)
Tel.: +34 91 374 60 00 y +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com