La Comisión Europea cifra en 400.000 millones el coste anual de los ataques informáticos para la economía mundial.

El camino hacia la conciencia digital

De la misma forma que los usuarios de nuevas tecnologías deben tomar conciencia de los riesgos asociados al uso de dispositivos móviles y servicios de internet, las empresas y organismos deben ser conscientes de que la transformación digital entraña riesgos de ciberseguridad y que es necesario adoptar medidas para evitarlos, atajarlos y recuperarse o responder ante ellos.

LUIS MENÉNDEZ
luis.menendez@yahoo.es

"LOS ciberataques pueden ser más peligrosos para la estabilidad de las democracias y economías que las armas y los tanques; no conocen fronteras y nadie es inmune", decía el entonces presidente de la Comisión Europea, Jean-Claude Juncker, en una presentación de nuevas herramientas para luchar contra ciberataques en el marco del Estado de la Unión de 2017.

Los ataques con programas de secuestro se han triplicado entre 2015 y 2017, según datos de la Comisión Europea, que cifra en 400.000 millones el coste anual de los ataques informáticos para la economía mundial. Por su parte, 9 de cada 10 europeos consideran la *ciberdelicuencia* como un desafío importante para la seguridad interior de la UE. Esta preocupación es compartida por la UE, que ha incluido esta problemática entre sus principales prioridades para el período 2018-2021, encaminando sus pasos a mejorar su respuesta a los ataques informáticos dirigidos contra los Estados miembros o instituciones de la UE.

Los incidentes de seguridad son cada vez más frecuentes y complicados de resolver y pueden

Hoy en día, las empresas y organismos trabajan bajo la premisa de que antes o después van a sufrir un ciberataque, por eso la clave es intentar anticiparse

Otros enfoques, mismo tema

▶ En este artículo de la revista *Unir*, Diego Caldentey aborda el concepto de industria 4.0, la importancia de la ciberseguridad y los motivos por los que España es la mayor industria de ciberseguridad industrial del mundo.
▶ https://cutt.ly/0ezAdn1

▶ En el documento *Ciber-Resiliencia: Aproximación a un marco de medición*, el Centro de Respuestas a Incidentes de Seguridad CERT del Incibe propone un marco de medición de indicadores dirigido a medir la capacidad de las organizaciones ante distintos ataques, amenazas o incidentes que puedan sufrir.
▶ https://cutt.ly/VezSuaF

▶ En esta sección web, el Consejo Europeo repasa cronológicamente las medidas de carácter normativo adoptadas para luchar contra la *ciberdelincuencia*.
▶ https://cutt.ly/KezS55X

afectar tanto a empresas como a servicios públicos, lo que, por extensión, puede dañar la confianza de los consumidores. Por ello, los esfuerzos se han dirigido, por una parte, a reforzar la legislación para responder de forma más eficiente a esta amenaza creciente. Así, el pasado mes de abril el Consejo Europeo adoptó el Reglamento sobre Ciberseguridad, que introduce la Agencia de la UE para la Ciberseguridad, creada para mejorar y sustituir a la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (Enisa, por sus siglas en inglés).

Este nuevo enfoque normativo implica, asimismo, la creación del Centro Europeo Industrial, Tecnológico y de Investigación en Ciberseguridad, que estará respaldado por una Red de Centros Nacionales de Coordinación, con el objetivo de ayudar a proteger el mercado único digital y a incrementar la autonomía de la UE en el ámbito de la ciberseguridad.

El siguiente paso de la UE ha sido establecer un marco que le permitiera "imponer medidas restrictivas específicas para disuadir y contrarrestar los ciberataques que representen una amenaza exterior para la UE o sus Estados miembros", en particular los efectuados contra

La UE se pone seria

La Unión Europea podrá imponer sanciones a las personas o entidades que estén detrás de *ciberataques* (o tentativas), a quienes presten apoyo financiero, técnico o material, a quienes estén implicadas de algún otro modo, así como a las personas y entidades asociadas con ellas. Entre las medidas restrictivas previstas se encuentra la inmovilización de activos de dichas personas y entidades y la prohibición de viajar a la UE.

Sparta: seguridad cibernética

OTRA línea de actuación de la UE en materia de ciberseguridad son los proyectos de investigación. Uno de ellos es 7, una red de competencia en seguridad cibernética, financiado por la UE con 16 millones de euros a través de su programa Horizonte 2020, cuyo objetivo es desarrollar y poner en funcionamiento acciones colaborativas de investigación e innovación.

En el proyecto trabajan 44 empresas y organismos de 14 Estados miembros de la UE, dirigidos por la Comisión Francesa de Energías Alternativas y Atómica (CEA), que aspira a crear la red más potente de competencias en ciberseguridad del continente. Cuatro de estos 44 actores trabajan desde España: Eurecat, Tecnalia, Vicomtech e Indra. Esta última trabaja para dotar de "capacidades avanzadas de consciencia situacional, imprescindibles para saber lo que ocurre en las redes y responder ante amenazas", señala la multinacional.

terceros Estados u organizaciones internacionales, si esas medidas se consideran necesarias para alcanzar los objetivos de la política exterior y de seguridad común.

La clave es ser consciente. Pero, ¿qué es la *ciberconsciencia*? Los términos *ciberconsciencia*, conciencia situacional o conciencia digital aluden a una misma realidad. Actualmente, los consumidores de nuevas tecnologías tienen a su alcance dispositivos muy potentes con los que pueden hacer infinidad de cosas, pero su uso conlleva riesgos de los que es necesario ser consciente. Por ejemplo, de que por el hecho de no tener que pagar dinero necesariamente por usar servicios de internet o aplicaciones, esto no tenga un coste, ya que la moneda son los datos, con los que se elaboran perfiles personalizados a partir de gustos e intereses.

Es imprescindible educar a los menores en el uso responsable de internet y las nuevas tecnologías, para que sepan que acosar a un compañero/a utilizando un *smartphone* puede tener consecuencias penales, al igual que para quien reenvía un contenido de tipo violento o sexual sin el consentimiento del afectado, con independencia de su edad. El uso de *wifis* públicas o de aplicaciones para ligar también pueden llevar aparejados riesgos de los que hay que ser consciente. La conciencia es conocer el contexto de los riesgos en función de la herramienta utilizada y el uso que se hace de ella.

El concepto es igualmente válido para las empresas. La conciencia digital implica ver los pros y los contras de actuar de una forma u otra en función de los riesgos. En el caso de la transformación digital de empresas y organismos también implica tomar conciencia de los riesgos que aquella representa para la ciberseguridad.

Anticiparse. Hoy en día, las empresas y organismos trabajan bajo la premisa de que antes o después van a sufrir un ciberataque, por eso la clave es intentar anticiparse. Atrás quedó el enfoque tradicional de poner barreras de protección (antivirus). Actualmente, además de poner muros, se analiza si existen patrones de comportamiento que podrían suponer un riesgo y también se trabaja la capacidad de respuesta.

Las empresas están destinando parte de sus inversiones a articular procedimientos y mecanismos para resolver posibles incidentes en el menor tiempo y hacer la empresa más resiliente. Por tanto, están trabajando de forma preventiva –intentando anticiparse– y en la parte post –presuponiendo que los malos van a entrar o ya han entrado– y actuar rápidamente para recuperar la información.

El uso de la inteligencia artificial, *big data* y *data analytics* es una de las tendencias que se trabajan en la fase preventiva. El volumen de información que se maneja es de tal magnitud que ha pasado a considerarse básica la utilización de estas tecnologías para detectar posibles patrones de comportamiento. No se trata solo de analizar esa cantidad ingente de información sino de poderla cruzar con otras fuentes, de forma que se puedan obtener o inferir datos de valor que permitan saber si la amenaza existe o no.

Muchas aplican la *ciber-resiliencia*, que es la capacidad de recuperarse ante un incidente de seguridad. Ante un ataque a un portal web, por ejemplo, sería el tiempo que se tarda en volver a la normalidad y lograr que funcione al cien por cien. Si el ataque fuera la difusión de una noticia falsa que dañara la reputación de una empresa, la *ciber-resiliencia* consistiría en recuperar nuestra credibilidad y no solo en lograr que eliminen la noticia o dejen de difundirla. ●

Nueve de cada diez europeos consideran la ciberdelicuencia como un desafío importante para la seguridad interior de la UE

DAVID FERNÁNDEZ GRANADO,
Head of Cyber Security Business de Minsait, una compañía de Indra

La ciberseguridad como un viaje

VIVIMOS en un mundo donde los cambios son cada vez más rápidos y en el que la incertidumbre alimenta la realidad. Un mundo marcado por la digitalización, que transforma la sociedad provocando la aparición de nuevas oportunidades, pero también riesgos que debemos evaluar, cuantificar y gestionar, lo que sitúa a la *ciberseguridad* en el centro de dicha transformación.

La *ciberseguridad* ha existido desde la aparición de las tecnologías de la información, aunque se la ha ido conociendo bajo diferentes nombres: seguridad informática, seguridad de red, seguridad de la información…. Pero, ¿cuál es la novedad que ha marcado la relevancia de la *ciberseguridad* hoy en día? La respuesta es sencilla: la velocidad de los cambios.

Hace diez años se abordaba el problema de seguridad de la información haciendo un análisis de riesgos, viendo el impacto que podía tener en los activos de información que sustentaban el negocio y elaborando un plan priorizado en base al riesgo para el negocio para el cual nos dábamos de entre dos a cinco años para ejecutarlo. Hoy esto es impensable.

La realidad cambia tan rápido que debemos evaluarla y reevaluarla frecuentemente situando los ciclos de evaluación y ejecución en no más de tres meses. Esto supone un verdadero reto para las empresas, la sociedad y los gobiernos que se han visto envueltos en una *Cyber Revolution* para la cual no estaban preparados.

Las claves de este cambio rápido son:

- Los negocios digitales y la sociedad digital cambian muy rápido y son globales. De igual manera lo hacen las amenazas.
- Las regulaciones en el ámbito digital proliferan muy rápido.
- Los *cyber malos* siempre persiguen el dinero.

No podemos cambiar esta realidad. Pero sí podemos variar cómo la afrontamos cada uno desde nuestro ámbito de responsabilidad, teniendo en cuenta que la *cyber evolution* que proponemos no es un destino, sino que es un viaje en sí mismo.

Analicemos las diferentes etapas del viaje tomando como ejemplo una amenaza de actualidad y que afecta a la vida personal y familiar: el *cyberbulling*.

Existe una primera fase que denominaremos "Denial". Tal y como sucede en otros ámbitos de la vida, cuando cambia la realidad de forma brusca y nos saca fuera de nuestra zona de confort, solemos tener una reacción de negación de dicha realidad. Aterrizando esto en un ejemplo todos los días podemos ver en los medios de comunicación cómo el uso inadecuado de redes sociales por parte de menores les pone en riesgo. Una de las primeras reacciones es pensar que ese tipo de situaciones no les van a suceder a nuestros hijos. Ahí es donde comienza nuestro problema.

La fase "Worry" está definida por un efecto rebote. Siguiendo con el ejemplo, cuando alguien cercano sufre acoso a través de redes sociales pasamos de la negación a la preocupación y tendemos a sobre reaccionar. Nos ocupamos de conseguir todos los artilugios tecnológicos que creemos necesarios pero nos olvidamos de educar y/o concienciar.

La que denominaremos *False Confidence* es la etapa en la que pensamos que hemos terminado el viaje. Que ya estamos listos para evitar la amenaza y consideramos que estamos 100% seguros. Al contrario, es entonces cuando más expuestos a la amenaza estamos. Siguiendo con el caso que analizamos como ejemplo, puede ocurrir que hayamos decidido retirarle el móvil a nuestro hijo, pero eso no elimina la amenaza.

Hard Lessons es el momento más difícil del viaje es en el que nos damos cuenta que el 100% de seguridad no existe y pensamos que no podemos hacer nada. Algo que, evidentemente, no es cierto: podemos minimizar el impacto de la amenaza si esta se produce gestionando adecuadamente el incidente, así como aprender para que no vuelva a suceder, al menos, el mismo caso.

Y finalmente, nos encontramos con la etapa de *True Leadership*. En ella, logramos alcanzar la madurez que supone asumir que la *ciberseguridad* es cosa de todos. Y hemos entendido que para minimizar el riesgo del ejemplo que estamos tratando debemos concienciar y educar, no solo a nuestros hijos, sino a la familia, al colegio/instituto y en general a la sociedad. La responsabilidad es compartida y se deben coordinar esfuerzos para reducir el riesgo.

Una vez entendido el viaje y sus fases con un ejemplo cercano, nos resultará más sencillo aplicarlo a un contexto de negocio digital. Nuestra aspiración también debe ser llegar a la etapa de "True Leadership" y eso no se puede hacer de la noche a la mañana. Es un reto alcanzable, pero que requiere un cambio cultural importante. Todo pasa por entender en qué etapa del viaje está nuestro negocio, nuestra empresa o institución. Y visualizar el objetivo a corto, medio y largo plazo, priorizando en función de las necesidades del negocio y del riesgo que se quiera asumir.

«Todo pasa por entender en qué etapa del viaje esta nuestro negocio, nuestra empresa o institución»

Para abordar este viaje es necesario un guía experto que nos permita ir avanzando con paso firme. Esta es la figura del CISO (Chief Information Security Officer). Un perfil profesional que escasea, ya que los CISO deben presentar un perfil evolucionado, que no se enseña en las universidades actualmente, y que les permite cubrir una amplia gama de conocimientos diversos, que van desde el plano técnico (tecnología de soporte a la digitalización), pasando por el legal (regulaciones) y finalizando en el negocio.

Para finalizar, es necesario resaltar que, aun contando con el perfil de CISO que describimos anteriormente, la responsabilidad en *ciberseguridad* en una empresa o una institución es de todos los que la componen. Cada eslabón de la cadena de valor digital debe contribuir a minimizar los riesgos.

Adicionalmente, la *ciberseguridad* debe ser considerada como una oportunidad para los negocios en particular y para las economías nacionales e incluso europea en general, ya que facilitará la creación de un tejido productivo y de empleo de calidad en los próximos años.