

La ciberdelincuencia es un reto económico global



La ciberdelincuencia se ha convertido en los últimos años en uno de los retos económicos más importantes a **escala global**. El desarrollo de las nuevas tecnologías ha permitido que cada vez haya más información y más datos almacenados en la nube. Esta tendencia se ha incrementado, además, a causa de la pandemia de Covid-19.


El confinamiento

contribuyó a la expansión global del teletrabajo y a que buena parte de las relaciones sociales tuvieran que llevarse a cabo por internet.



Vivimos en una sociedad digitalizada y, aunque no somos consciente de ello, la seguridad de nuestras relaciones sociales y económicas se encuentra amenazada por la ciberdelincuencia.

La ciberdelincuencia como problema económico



Los delitos asociados con la ciberdelincuencia son muy variados, con una amplia diversidad de agentes y motivaciones. En este sentido, cabe señalar que existe una importante categoría de delitos difíciles de entender desde la lógica de la economía, como el ciberterrorismo o los ataques por motivos ideológicos o de venganza. En estos casos las motivaciones de los ciberdelincuentes están más relacionadas con aspectos psicológicos que con la búsqueda de beneficios económicos.

Aunque la ciberdelincuencia es una amenaza que afecta a todos los usuarios de internet, las empresas son las más perjudicadas debido, fundamentalmente, a los costes que genera. Así, por ejemplo, el ciberataque NotPetya, considerado el más nocivo de la historia, supuso para FedEx, empresa multinacional de mensajería que cotiza en la Bolsa de Nueva York, más de 300 millones de dólares en pérdidas.

El mismo volumen de pérdidas fue reportado por la naviera sueca Maersk como consecuencia del mismo ataque, que le obligó a paralizar parte de su cadena de producción durante semanas. En total, se estima que NotPetya causó pérdidas cercanas a los 10 mil millones de dólares en las empresas afectadas.

Pérdida de confianza de los clientes

El daño que genera la ciberdelincuencia a las empresas no se limita a los costes que tienen que afrontar por los negocios interrumpidos o para reparar los daños producidos. Las empresas afectadas por ciberataques se tienen que enfrentar al perjuicio que sufre su reputación en internet y a la pérdida de confianza de sus potenciales consumidores.



Un caso paradigmático es el ciberataque sufrido por la web de contactos extramatrimoniales Ashley Madison en 2015 por parte del grupo de hackers The Impact Team. Este ataque reveló 300 GB de datos personales de usuarios de la web, incluyendo datos bancarios, nombres reales e información íntima. Luego muchos usuarios fueron extorsionados por otros ciberdelincuentes, que exigían dinero a cambio de no revelar esta información a sus familiares. Precisamente por el daño en la reputación que supone para una empresa reconocer públicamente haber sido víctima de un ciberataque, muchos se mantienen en secreto e incluso no se denuncian.

Además del miedo a la pérdida de la confianza de sus clientes, existen otras causas que pueden explicar este comportamiento.

Una de ellas puede ser la desconfianza ante la capacidad de las fuerzas de seguridad nacionales para hacer frente a grupos criminales internacionales. Otra es la necesidad de retomar cuanto antes la actividad empresarial. Incluso si ello supone ceder a la extorsión de los ciberdelincuentes y pagar las cantidades que exijan para poder recuperar la normalidad en la empresa.



Factores determinantes de la ciberdelincuencia

La ciberdelincuencia constituye un fenómeno complejo, que engloba numerosas actividades muy diferentes que son llevadas a cabo por una amplia variedad de agentes. Por ello resulta difícil detallar sus causas, ya que son muy variadas y van desde factores personales, como la personalidad o ideología de los ciberdelincuentes, hasta fenómenos internacionales como la creciente globalización o la expansión de internet y las nuevas tecnologías.

Existen además otros factores que influyen sobre la ciberdelincuencia, como el marco regulatorio o el nivel socioeconómico de un país. Por ejemplo, Rusia o China no suelen colaborar con otros países en la investigación de los ciberdelitos que no afectan negativamente a sus intereses nacionales. De hecho, se han negado a firmar el Convenio de Budapest, único tratado internacional existente sobre ciberdelincuencia. Así, los ciberdelincuentes ven cómo sus acciones en el extranjero pueden quedar impunes, lo que crea un incentivo para continuar con su actividad delictiva. Las amenazas son globales, pero las leyes no lo son.



También se ha observado que muchos ciberdelitos surgen de países en vías de desarrollo con regulación limitada y altos índices de desempleo. En este sentido, es más probable que la ciberdelincuencia surja en países donde la mano de obra especializada en informática no encuentra oportunidades de empleo adecuadas para su nivel de formación. Es lo que ha ocurrido en Rusia y otros países del Este de Europa.

¿Cómo actuar ante este reto global?

En primer lugar, es fundamental contar con fuentes de información fiables sobre los ciberdelitos y su impacto económico. Es recomendable, además, que la información provenga de organismos independientes. Que los autores de las investigaciones sean empresas especializadas en ciberseguridad provoca desconfianza en la fiabilidad de sus datos.

En segundo lugar, la ciberdelincuencia es una actividad que se encuentra en constante innovación y transformación. Esto supone un grave problema tanto para las empresas de ciberseguridad como para las fuerzas de seguridad, que no pueden responder a la inmediatez de los cambios en los ciberdelitos.

En este sentido, aunque resulta muy difícil prever el futuro, existen no pocos motivos para la preocupación, especialmente por el desarrollo de la tecnología 5G y la inteligencia artificial. Aunque pueden contribuir

a mejorar la ciberseguridad económica también pueden ampliar enormemente las posibilidades de la ciberdelincuencia.

Cooperación internacional, intimidad personal

Los ciberataques son amenazas transnacionales que las fronteras de los países no pueden frenar. Para poder avanzar en este sentido sería necesario establecer fuertes lazos de cooperación entre países e instituciones, pero también con las empresas privadas.

Lamentablemente, es muy difícil alcanzar un grado efectivo de colaboración internacional y público-privada. Además, las medidas dirigidas a combatir los ciberdelitos y aumentar la seguridad de las redes pasan, en muchos casos, por recabar información personal de los ciudadanos, lo que puede ser considerado como una intromisión de su intimidad, dificultando, por tanto, su aplicación.

En definitiva, la ciberdelincuencia supone un importante reto para la gobernanza global. Mientras la amenaza no tiene fronteras, las instituciones y normas dirigidas a su control y erradicación se limitan a los territorios nacionales.

Por ello, es fundamental el establecimiento de instituciones reguladoras y normativas supranacionales que puedan dar una solución global a este problema.

Fuente de información: www.eleconomista.com.mx

Autora: María Teresa Aceytuno

