UNA REFLEXIÓN SOBRE CIBERSEGURIDAD Y RENTABILIDAD: ¿SON SEGURAS LAS INVERSIONES DE LA BANCA Y LOS FONDOS?

ALFONSO PASTOR, socio de LEET SECURITY

El despacho británico PGMBM ha abierto un proceso de demanda colectiva contra British Airways por el incidente sufrido en 2018. Un incidente por el que fueron expuestos los datos de nombres, direcciones y tarjetas de crédito/débito de 420.000 clientes, que podrían reclamar 2.000 libras cada uno, lo que supone que el importe global podría superar los 800 millones de libras, una cantidad equivalente al 50% de los beneficios que el grupo IAG obtuvo en 2019. Además de la sanción de 20 millones ya impuesta por el ICO (equivalente a nuestra Agencia de Protección de Datos). Este es un claro ejemplo de la importancia que debe otorgarse a la ciberseguridad a la hora de considerar una inversión.

Un posicionamiento inadecuado o deficiente puede conducir a incidentes de graves consecuencias que deterioren el valor de cualquier inversión tanto como una pandemia. Y no solamente se trata de aquellas compañías que manejan enormes cantidades de datos personales, aunque evidentemente en este tipo de empresas el régimen sancionador puede alcanzar proporciones enormes de hasta el 4% de la facturación global. Y es que un ciberataque puede tener efectos operativos desastrosos, como el ocurrido a la naviera Maersk tras el ataque con el ramsomware notPetya en 2017, que causó pérdidas a la compañía por 300 millones de dólares.

Y eso que estamos hablando de grandes organizaciones que cuentan con recursos, tanto financieros como de personal, y tienen una notable capacidad de recuperación. Pero no todas las inversiones son en compañías de gran tamaño. Precisamente las empresas más pequeñas son las receptoras de un mayor número de ciberataques, de los que podrían incluso no recuperarse.

Cuando se realizan inversiones en otras compañías, resulta de enorme importancia analizar su posicionamiento de ciberseguridad, para evitar en lo posible que estas se deterioren de forma contundente. No en vano, las grandes agencias de rating ya vienen anunciando desde

"CUANDO SE REALIZAN INVERSIONES EN OTRAS COMPAÑÍAS, RESULTA DE ENORME IMPORTANCIA ANALIZAR SU POSICIONAMIENTO DE CIBERSEGURIDAD, PARA EVITAR EN LO POSIBLE QUE ESTAS SE DETERIOREN DE FORMA CONTUNDENTE"

hace tiempo que los ciber riesgos pueden impactar directamente en las calificaciones crediticias.

Tras sufrir el citado ataque, Adam Banks, responsable de tecnología de Maersk, indicó en unas declaraciones que muchas de las medidas de seguridad habituales no son lo bastante robustas para tratar con este tipo de amenazas. Y los ciberseguros, aunque convenientes, no resultan suficientes, porque la prevención es la estrategia más efectiva.

¿Cómo puede saber un fondo de inversión si las medidas de ciberseguridad de una empresa son las adecuadas antes de invertir?

Por eso, aunque el presupuesto destinado a ciberseguridad que realizan las organizaciones está creciendo año tras año, su retorno es muy difícil de calcular, ya que siempre estará referido a los costes derivados de los potenciales incidentes que se pretenden evitar. Pero ¿cómo puede un fondo de inversión estar seguro de que las inversiones en medidas de ciberseguridad resultan efectivas? Una pregunta nada baladí, si tenemos en cuenta que un reciente informe del Instituto Ponemon muestra que más de la mitad de las organizaciones no saben si los recursos dedicados a la ciberseguridad están protegiendo realmente sus sistemas de información.

Resulta pues necesario realizar una detallada evaluación de la efectividad de los presupuestos empleados en seguridad por las organizaciones, que analice todos los factores que pueden afectar, tanto al nivel de protección, como a la capacidad de recuperación. El Instituto Nacional de Estándares de Seguridad, NIST, define para ello cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperarse, que deben ser tenidas en cuenta. Y no solo basta con examinar a nuestra organización conforme a estos criterios, sino que también debemos tener en cuenta a los proveedores de una empresa.

Alfonso Pastor,
socio de LEET Security

"EL SECTOR BANCARIO CONOCE BIEN LA IMPORTANCIA DE EVALUAR LA SEGURIDAD DE LOS PROVEEDORES"

Incidentes como el reciente de SolarWinds nos recuerdan que la seguridad de los proveedores es crucial, ya que estos pueden derivar a su vez en fugas de información o causar problemas operativos en el negocio de sus clientes.

Sector bancario

El sector bancario conoce bien la importancia de evaluar la seguridad de los proveedores, puesto que el regulador europeo, la EBA, establece en sus directrices sobre externalización el requerimiento de auditar la seguridad de todos aquellos servicios importantes para el negocio de las entidades (incluso realizando la evaluación con carácter previo a su contratación).

En este sentido, la banca española cuenta con una herramienta pionera: el servicio PINAKES, desarrollado por el Centro de Cooperación Interbancaria y LEET Security, que utiliza el sistema de calificación de ciberseguridad de LEET Security, para facilitar el cumplimiento de la normativa europea, aportar mayor eficiencia al sector y mejorar la seguridad de todo el sistema financiero, de lo que podrán beneficiarse todos los asociados al CCI.

Este modelo de calificación puede resultar una aportación equivalente al rating crediticio, cuando se trata de evaluar el posicionamiento y capacidades de ciberseguridad de una organización. Vital para asegurar la viabilidad de cualquier empresa. ■