S&P bajará el ráting a los bancos mal protegidos frente a los ciberataques

La amenaza de los ciberataques contra los bancos crece en paralelo al uso de las nuevas tecnologías y a la oferta digital.

Los bancos fortalecen sus defensas para proteger su negocio así como los datos y la confianza de sus clientes. Pero no solo deben hacerlo por eso. La agencia de ráting Standard & Poor's (S&P) les acaba de dar otra razón.

Si los bancos no están lo suficientemente blindados frente a los piratas informáticos la firma estadounidense les puede bajar la nota. «Vemos la débil seguridad frente a los ciberataques como una amenaza emergente que puede suponer un riesgo más alto para las entidades financieras en el futuro, y posiblemente dar lugar a rebajas de calificación», anticipa.

El analista de S&P Stuart Plesser subraya en un reciente informe que los bancos son la diana permanente de los delincuentes cibernéticos debido al gran valor de los datos que atesoran, a la elevada interconexión del sistema financiero y a su papel como conductos de divisas.

La agencia considera que por ahora el riesgo de crédito derivado de los ciberataques es «medio» y que los grandes bancos ya han dado pasos adecuados para mitigar los riesgos conocidos. Sin embargo, advierte de que la amenaza de ciberataques es creciente y que si un banco no logra repeler un ataque maligno «puede sufrir importantes daños tanto económicos como legales y de reputación».

La firma explica que no ha bajado los ráting de los bancos que han sufrido violaciones de sus sistemas de seguridad en los últimos años porque los daños no han sido graves. JPMorgan sufrió un ataque que comprometió la información de decenas de millones de clientes, pero los datos «eran de bajo nivel, no contenían los números de la seguridad social», alega.

«Si creemos que un banco está mal preparado para encarar un ciberataque, podríamos bajarle el ráting antes incluso de que lo sufra. La bajada también puede producirse después de una violación del sistema de seguridad si estimamos que ha provocado daños de reputación significativos que podrían derivar en la pérdida de clientes, o si las pérdidas económicas o legales dañan el capital», afirma.

Pocos bancos dan a conocer los costes de sus sistemas de ciberseguridad como ha hecho JPMorgan, que ha aumentado en un 80% el presupuesto en los próximos dos años, hasta 450 millones de euros, iniciativa que S&P aplaude. De cara a su evaluación de los ráting, la firma ya ha empezado a preguntar a los bancos si están aumentando el gasto en defensas frente a los piratas informáticos.

Su cuestionario también indaga sobre la experiencia del consejo de administración frente a los ciberataques, si el banco tiene algún tipo de seguro para encarar este riesgo, cuánto tiempo tarda habitualmente en detectar una agresión, qué procedimientos activa tras una detección, cuáles son sus zonas más vulnerables o si realiza ejercicios de estrés para medir su resistencia.

Tipos de piratas informáticos

S&P resalta que hay muchos tipos de piratas informáticos con el denominador común de tener a los bancos en su punto de mira. Los grupos criminales, las organizaciones terroristas y los hackers buscan obtener un beneficio económico. Otros quieren dañar a los bancos con independencia del rédito pecuniario por su pertenencia a un país que consideran enemigo o para promover una ideología, como en el caso del os activistas.

De hecho, los ataques procedentes de países-estados hostiles son la amenaza más sofisticada a la que se enfrentan los bancos y su riesgo aumenta en paralelo a las tensiones políticas. Según S&P, si un estado-nación hostil centra sus esfuerzos en un ataque a un banco «probablemente tenga éxito», por lo que tras una primera línea de defensa, las entidades deben redoblar esfuerzos para acelerar sus respuestas ante las fisuras que detecten en sus sistemas de seguridad y en aislar la parte que aún no se ha visto comprometida.

Por eso los servicios de inteligencia de Estados Unidos trabajan de cerca con los bancos cuando las tensiones políticas crecen y pueden dar lugar a represalias de un estado-nación hostil. La UE, por su parte, desarrolla una directiva sobre la seguridad de las redes y la información que -de implementarse en su estado actual- articula la forma de cooperación y de compartir información entre instituciones oficiales y los bancos, así como protocolos de respuesta ante emergencias.

El espionaje industrial que busca el robo de información confidencial -como los detalles sobre una fusión o compra- es otro tipo habitual de ataque ante el que los bancos deben protegerse, junto al de aquellos trabajadores insatisfechos que dejan la compañía tras haber accedido a información sensible o relacionada con el sistema de seguridad.

Fuente: http://www.expansion.com/empresas/banca/2015/10/07/56158a70ca4741fb468b45ae.html