computing
www.computing.es

1 June, 2017

EL 78% DE LOS CISOS CONFIAN EN LA SEGURIDAD DE SUS EMPRESAS

La banca necesita integrar el riesgo cibernético en su estrategia global de operaciones

Los bancos son cada vez más conscientes de las amenazas que los delitos cibernéticos representan para su negocio y trabajan continuamente en mejorar sus defensas y en incrementar la sensibilización de su personal.

Una investigación publicada por Accenture ha hallado que el 78% de los altos directivos responsables de seguridad confían en la estrategia de ciberseguridad de sus compañías. Sin embargo, quizá estos ejecutivos sean demasiado confiados, puesto que, según el mismo informe, de entre los miles de ataques de phishing, malware y similares que reciben las empresas del sector cada año, una media de 85 son de carácter grave; y de estos, aproximadamente un tercio (el 36%) logra su objetivo, lo que significa que obtienen cierta información de la compañía.

Para hacer frente a estas amenazas, se requieren planteamientos innovadores en términos de ciberseguridad. Tradicionalmente, la banca ha establecido controles de gestión del riesgo cibernético en sentido descendente, con un perímetro de seguridad. No obstante, en la actualidad se debe lidiar con las complejidades de firewalls, malware y phishing y con un mayor uso de prácticas de ingeniería social; así, el sector está encontrando serias dificultades para conectar los aspectos técnicos de la ciberseguridad con otras cuestiones más amplias dentro del riesgo operacional, definido por el Comité de Basilea como "el riesgo de sufrir pérdidas debido a la inadecuación o a fallos en los procesos, personal y sistemas internos o bien por causa de eventos externos".

Hay que tener en cuenta que tanto los empleados, como los procesos y la tecnología pueden verse afectados por un ciberataque; y que, tras este, los bancos no solo deben lograr que sus sistemas informáticos vuelvan a ponerse en funcionamiento rápidamente, sino que también tienen que tranquilizar a clientes y reguladores, implementar sistemas de refuerzo efectivos y, probablemente, compensar pérdidas. Todo ello exige una planificación previa, cooperación y comunicación entre los equipos de operaciones, riesgos, infraestructuras y ciberseguridad. Por tanto, la correcta planificación es esencial para la estrategia de defensa de las empresas y por ello debe ser priorizada en función del riesgo.

Otro factor es la rapidez de poner bajo cuarentena un área que ha sido atacada, para permitir que el resto de sistemas y procesos del banco continúen operando mientras se investiga el área afectada, se rehabilita y se vuelve a poner en servicio. Incorporar la estrategia de riesgo cibernético al sistema de gestión del riesgo empresarial (ERM) contribuye a reducir el daño de una pérdida de información, de un ataque de denegación de servicio distribuido (DDoS) o de otros incidentes de este tipo.

De igual modo, la banca continúa intensificando sus inversiones en ciberseguridad y su enfoque de protección basado en el riesgo. Además del gasto en tecnología y en expertise informático, las compañías también están dirigiendo sus esfuerzos hacia la mejora de sus estructuras, con el objetivo de crear una cultura de la seguridad más cohesionada. Si el programa de seguridad de una compañía se apoya e integra en una estrategia de riesgo y de negocio exhaustiva, se podrá implementar un 'programa de respuesta cibernética' completo, que incluya la comunicación con stakeholders y la protección y recuperación de los activos clave. Así, el banco disminuirá su exposición al riesgo a la vez que mejorará la velocidad y efectividad de sus respuestas.

Las amenazas cibernéticas continuarán evolucionando, por lo que solo aquellos bancos que incluyan sus esfuerzos en ciberseguridad dentro de sus estrategias globales de riesgo operacional serán resilientes en este entorno tan exigente. ■

FERNANDO RUFILANCHAS |
Managing Director Financial Services Accenture España, Portugal e Israel

"La banca continúa intensificando sus inversiones en ciberseguridad y su enfoque de protección basado en el riesgo"