EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
21.01.2015	Dinero	14

Soberanía de datos, el próximo conflicto

GUARDAR INFORMACIÓN EN SERVIDORES QUE PUEDEN ESTAR EN OTROS PAÍSES PLANTEA UN PROBLEMA LEGAL

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

Las mayores preocupaciones de las empresas se relacionan con el flujo de efectivo, la expansión o hasta los ataques informáticos; sin embargo es momento de que presten atención a temas que pueden generar conflictos, como la soberanía de datos, encriptación de la información y la privacidad.

Para Marcelo Bezerra, director de Ingeniería del área de Seguridad para América Latina de Cisco, esta época ha sido marcada por las filtraciones del exanalista Edward Snowden acerca de la vigilancia de la Agencia Nacional de Seguridad de Estados Unidos sobre sus propios ciudadanos y otros gobiernos, ataques informáticos, como el ocurrido a Sony Pictures en 2014 o hasta el reciente atentado a la revista satírica francesa *Charlie Hebdo*.

"Lo que pasa en el escenario geopolítico puede tener un impacto directo en las cadenas de suministro global y en cómo el negocio administra la información de los clientes y los empleados en diferentes países".

Además la necesidad de los gobiernos de vigilar más internet y mantener protegida la información de las personas podría derivar en nuevas leyes o regulaciones, lo que generará costos para las empresas, particularmente las multinacionales.

Cosa de leyes

Al presentar el reporte *Seguridad Anual Cisco 2015*, Bezerra comentó que gracias al uso del cómputo en la *nube* (servidores remotos) y tendencias como el internet de las cosas, mucha de la información de gobiernos y empresas se almacena o procesa en servidores que pueden estar en otros países, situación que a la larga supondrá un problema.

"Si una empresa de Estados Unidos contrata un servicio y su banco de datos se almacena en un servidor en India y se hace el respaldo en otro que se encuentra en México, ¿quién tiene la soberanía de esos datos?", reflexionó.

El problema para las empresas y gobiernos es saber qué ley aplicar a esa información y determinar qué autoridad puede revisarla en casos extremos.

Lo anterior ha provocado que se planteen iniciativas para que todo tipo de información sea encriptada de punto a punto, para así evitar problemas de soberanía o de vigilancia.

Países como Reino Unido rechazan la encriptación porque reduce la transparencia y podría beneficiar a los cibercriminales.

Otra opción es que datos sensibles de los clientes y empleados sea almacenada en servidores nacionales, sin embargo esto no asegura que tenga un respaldo o evita intrusiones.

Bezerra y Ghassam Dreibi, gerente de desarrollo de negocios de seguridad para América Latina de Cisco, coincidieron en que Naciones Unidas debe hacer un esfuerzo para crear un consenso sobre la privacidad y otros temas para regular internet sin retroceder en la libertad de expresión.

Sin consenso

Por separado, cada país está tomando medidas para proteger a los usuarios de la red y a las empresas. Por ejemplo, Brasil creó el año pasado su primera Ley de Internet, México promulgó una reforma en la Ley de Telecomunicaciones, Colombia cuenta con diferentes regulaciones y en Argentina está en discusiones una nueva norma.

"No vemos que América Latina pueda crear un bloque y hacer reglas iguales para todos como la Unión Europea, no vemos una madurez o un nivel de comunicación para hacerlo", dijo Dreibi.

Empresas no conocen sus debilidades

Cisco advirtió que en las empresas alrededor del mundo existe una brecha entre la percepción y la realidad de lo que está sucediendo en materia de seguridad informática, lo que genera áreas de oportuni-

Continúa en siguiente hoja


HACKER
Soberanía de datos, el próximo conflicto
Facebook aporta 200 mil mdd a la economía

EXCELSIOR
EL PERIÓDICO DE LA VIDA NACIONAL

Fecha	Sección	Página
21.01.2015	Dinero	14

dad para los cibercriminales.

De acuerdo con el *Reporte de Seguridad Anual Cisco 2015*, el 90 por ciento de las casi mil 700 empresas encuestadas confían en sus políticas y procesos para proteger sus redes, lo que contrasta con el hecho de que al menos 54 por ciento de éstas ha tenido que soportar el escrutinio público como consecuencia de una brecha en su seguridad.

Marcelo Bezerra, director de ingeniería del área de seguridad para América Latina de Cisco, indicó que esta brecha entre la percepción y la realidad también se observa al hablar con los Jefes de Seguridad de la Información de las compañías porque el 75 por ciento asegura que su plataforma es eficiente, pero menos del 50 por ciento de los ejecutivos de operaciones no concuerda con ellos.

Esta situación ha provocado, consideró el director de la tecnológica, que las empresas no estén utilizando sus presupuestos para seguridad de manera eficiente y dejen puertas abiertas a los cibercriminales.

"Las empresas siguen invirtiendo mucho en seguridad, pero su punto más flaco sigue siendo sus empleados", destacó.

Corrientes como el "internet de las cosas" y "trae tu propio dispositivo" provocan que los empleados conecten sus equipos a la red empresarial, sin saber si están infectados por algún código malicioso que bajaron de la red sin percatarse.

Bezarra comentó que esa es la manera más fácil de atacar una empresa, primero contaminar el equipo de un empleado y así llegar a la red para entonces usar métodos más sofisticados para robar información y venderla en el mercado negro o usarla como soborno.

Además las propias empresas no prestan atención a las reglas más básicas de protección, ya que 56 por ciento no ha actualizado sistemas como OpenSSL que fue el origen de la vulnerabilidad conocida como Heartbleed.

"Los usuarios siguen accediendo a correos de desconocidos, entran a páginas poco confiables y tienen sistemas sin actualizar", añadió.

–Aura Hernández