El riesgo de ciberataques, una realidad palpable

Diciembre 2018

LOCKTON®

Se dice, y con razón, que hay dos tipos de motociclistas: los que ya se cayeron de la moto y los que se van a caer. Así, la delincuencia en el ámbito de la tecnología es tan sofisticado que hoy podríamos igualmente decir que hay dos tipos de empresas, las que sufrieron un ciberataque y las que lo van a sufrir.

Tal vez suene exagerado, pero lo cierto es que hay casos recientes, a escala global y a nivel local (Facebook, Banco de México…), que nos permiten advertir que el riesgo de un ataque cibernético es una realidad inevitable.

Autor:

Gonzalo Herrasti
Productor
Lockton México
gherrasti@mx.lockton.com

¿Cuántos correos del área de Tecnología de la Información de nuestra empresa recibimos cada mes, advirtiendo que no abramos correos electrónicos dudosos? Y sólo pensamos en la "paranoia" de nuestros compañeros ingenieros de Sistemas.

Imaginemos un caso concreto, el de una compañía con operaciones en México, que en realidad podría ser cualquier empresa en la que trabajamos. Un colaborador de nivel mando medio no siguió las recomendaciones que enviaba constantemente su área de Tecnología de la Información sobre no abrir correos electrónicos de dudoso remitente. Al abrirlo, sin darse cuenta, automáticamente se contaminó su computadora afectando a muchas de las que estaban conectadas en esa misma red. El colaborador siguió trabajando, y mientras lo hacía, se perpetraba un acto malicioso por terceros, quienes lograron tener acceso a la información de la empresa; Por varios días, los hackers estuvieron grabando las actividades de los colaboradores que se conectaban a esa red, hasta llegar al área de Tesorería, en donde estaba guardada la información de las cuentas bancarias de la empresa.

Una semana más tarde los piratas cibernéticos secuestraron los datos y dejaron a la empresa 48 horas sin poder operar, ya que todo el sistema estaba tomado y pedían una cantidad de dinero muy semejante a la que tenía la empresa en inversiones.

Lo anterior fue posible porque durante varios días los delincuentes siguieron los movimientos bancarios de la empresa.

Después de 24 horas de negociaciones y el pago de una importante suma de dinero para recuperar sus sistemas y la información, todo parecía que regresaba a la normalidad, hasta que se percataron que la información que tuvieron secuestrada se vendió a la competencia, en donde ésta logró conocer el desarrollo de nuevos proyectos, las campañas que iban a implementar a corto y mediano plazo y la base de datos de los clientes.

Pero eso no fue todo, los piratas cibernéticos además pusieron en venta información bancaria de los clientes, por lo cual a varios de ellos les clonaron sus tarjetas de crédito, provocando demandas hacia la empresa por el incumplimiento del Aviso de Privacidad de datos en el cual prometían resguardar y hacer el mejor uso de esta información sensible.

Por si fuera poco, esto derivó en una multa por parte del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI).

Sin duda la reputación de esta empresa se vio severamente afectada, generando el inicio de un concurso mercantil por las bajas ventas en el último trimestre, dejando sin ingreso a varias familias.

El caso aquí detallado, aunque hipotético, bien podría ser uno de los 25 mil millones de intentos reales de intrusión a las empresas que en efecto han ocurrido en el último año, buscando vulnerar los sistemas para poder tener acceso y comprometer la valiosa información que se resguarda en cada uno de los equipos y sus nubes.

Ninguna empresa está exenta de padecer este tipo de ciberataques. En lo que va del 2018 los delitos y amenazas de este tipo han aumentado 215% en comparación con el año pasado.

México es el tercer país con más ciberataques en el mundo, sólo detrás de Estados Unidos y el Reino Unido. La pérdida estimada en México sólo en 2017 es de 7.7 mil millones de dólares como consecuencia de ciberataques informó la Procuraduría General de la República.

Casos recientes… y cercanos

¿Son casos aislados? ¿Difícilmente ocurriría en mi empresa? Error pensar así. Ha habido casos tan recientes como el de abril de este año, cuando cinco entidades bancarias mexicanas fueron hackeadas a través de su plataforma SPEI, lo que les produjo una pérdida aproximada de 300 millones de pesos, informó Banxico. Como parte de las consecuencias, algunos clientes no pudieron recibir su pago de nómina ni realizar movimientos de SPEI.

El 28 de septiembre de 2018 Facebook y 50 millones de sus usuarios fueron víctimas de un ciberataque que comprometió su información sensible, como correos electrónicos y contraseñas según reportó The New York Times.

Prevalencia, afectaciones… y multas

De acuerdo con los datos del último informe de la firma eslovaca de seguridad cibernética ESET, siete de cada diez empresas mexicanas han experimentado un incidente relacionado con seguridad informática.

Del 2012 a 2015, el INAI ha impuesto multas por más de 185 millones de pesos debido a violaciones a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Los sectores con mayor número de multas son los servicios financieros y seguros, medios masivos de comunicación y el educativo.

Datos ofrecidos por Norton (filial de Symantec, líder global en ciberseguridad de última generación), en el Cyber Security Insights Report 2017, señala que en ese año la pérdida fue de 172 billones de dólares a nivel mundial.

En 2017 el virus “WannaCry” afectó a más de 200 mil computadoras y 150 países alrededor del mundo. Dmitry Bestuzhev, director del equipo de Investigación y Análisis para Kaspersky Lab (una compañía internacional con sede en Moscú, dedicada a la seguridad informática con presencia en aproximadamente 200 países), informó que el país más afectado en América Latina fue México, seguido por Brasil y Ecuador.

Los riesgos

Los principales riesgos que existen hoy en día por un ciberataque son:

- Robo de datos de usuarios
- Pérdida o eliminación de información
- Robo de identidad
- Fraude o extorsión
- Secuestro de información
- Robo de Propiedad Intelectual
- Interrupción de servicios
- Multas por organismos regulatorios
- Daño a la Reputación

¿Cómo prevenir, reaccionar y amortiguar daños?

Vistos los daños que puede ocasionar un ataque cibernético a cualquier empresa, la pregunta es, ¿se puede hacer algo ante ello? La respuesta es Sí. **Existen seguros que cubren a la empresa ante este tipo de delincuencia, el llamado cyber crime.**

Las compañías, después de un ataque a sus sistemas informáticos establecen estrategias encaminadas a darle continuidad al negocio, entre las cuales se encuentran recuperar la información, resarcir la pérdida de ingresos por interrupción del negocio, volver a las actividades normales, reemplazar equipos dañados, mejorar en el tiempo la reputación de la empresa para volver a ganar la confianza, hacer frente a las demandas y multas, gastos forenses, etc. Lo anterior genera un costo muy alto que puede representar para algunas empresas la salida del mercado.

Por ello cada vez más es necesario contar con las medidas preventivas, de seguridad de la información y de continuidad del negocio, pero también contar con la protección financiera suficiente para resarcir los daños causados por un ciberataque. Es recomendable contar con la consultoría adecuada para evaluar las áreas vulnerables de la empresa, construir una estrategia con el área de Tecnología de la Información para que, en el momento de un incidente, se tengan los recursos necesarios para detectar y controlar la fuga de información y proteger datos sensibles, un equipo de abogados especializados para defender a la empresa de cualquier demanda, un equipo de ajustadores expertos en ciberataques para detectar amenazas y especialistas en Relaciones Públicas para limpiar la imagen y tratar de volver a la normalidad.

- ¿Cuentas con un plan de continuidad de tu negocio?
- ¿Conoces todas tus vulnerabilidades?
- ¿Sabes cada cuánto actualizan los niveles de protección de tu empresa?
- ¿Tu equipo está capacitado ante este tipo de incidentes?

Si en alguna de las últimas preguntas respondiste no, acércate con los expertos de Lockton, el corredor y consultor privado de seguros más grande del mundo.

- Nuestra experiencia en la cobertura de riesgos y ataques cibernéticos ha sido reconocida en importantes certificaciones mundiales. Por ejemplo, el equipo Cyber de Lockton en Londres fue galardonado por sus iniciativas innovadoras con el “Cyber Brokerage Firm of the Year”, en 2017. En 2015, Lockton obtuvo el reconocimiento “Best Cyber Risk Broking Team” en los Cyber Risk Awards, de la firma Advisen.
- Las alianzas de Lockton con grandes firmas como Cybernance Corporation y BitSight Security Ratings permiten ofrecer a sus clientes las mejores herramientas de seguridad. En Lockton construimos soluciones a la medida de tus necesidades. Contáctanos.

Fuentes:

1. “México, el tercer país con más ciberataques en el mundo”, publicado en Excélsior, 22 de noviembre de 2018.
   - https://www.excelsior.com.mx/hacker/mexico-el-tercer-pais-con-mas-ciberataques-en-el-mundo/1279944
2. “2017 Norton Cyber Security Insight Report” https://us.norton.com/cyber-security-insights-2017
   - https://us.norton.com/cyber-security-insights-2017
3. “7 de cada 10 empresas en México son víctimas de delitos informáticos”, publicado en The IT Mag, 8 de mayo de 2017
   - https://www.the-emag.com/theitmag/blog/7-de-cada-10-empresas-mexicanas-v%C3%ADctima-de-incidentes-de-ciberseguridad
4. “200 mil computadoras afectadas y contando en histórico ciberataque”, publicado en El Financiero, con información de la agencia Bloomberg, 15 de mayo de 2017
   - http://www.elfinanciero.com.mx/tech/ransomware-afecta-a-100-mil-computadoras-en-150-paises
5. “Inai impone multas por más de 185 mdp”, publicado en El Universal, 22 de diciembre de 2015
   - https://www.eluniversal.com.mx/articulo/nacion/politica/2015/12/22/inai-impone-multas-por-mas-de-185-mdp
6. “Perspectiva de ciberseguridad en México”. McKinsey & Company y COMEXI, junio de 2018.
   - https://consejomexicano.org/multimedia/1528987628-817.pdf

Misión | Ser la empresa de valor y servicio líder a nivel mundial en corretaje de seguros, administración de riesgos y servicios actuariales.

Objetivo | Ser el mejor lugar para hacer negocios y trabajar.

Lockton México
Avenida Santa Fe 481, piso 19
Colonia Cruz Manca
Cuajimalpa, Ciudad de México
C.P. 05349
T: +52 (55) 5980-4300

LOCKTON®
LOCKTON.COM.MX