Alto costo por no tener seguridad informática

Las **pérdidas económicas a consecuencia del cibercrimen** pueden ser bastante dolorosas para una empresa por no contar con una buena plataforma de seguridad informática, como sucedió con el sistema bancario mexicano hace unas semanas.

A inicio de mayo se dio a conocer la noticia de que al menos **300 millones de pesos y una mayor regulación a las operaciones mayores a 50 mil pesos fueron el saldo,** hasta ahora, de un ciberataque al software que usan las instituciones financieras en el país para conectarse al Sistema de Pagos Electrónicos Interbancarios (Spei) del Banco de México (Banxico).

El **ataque cibernético** que sufrieron algunas instituciones financieras afectó su proceso de conexión con el Spei, lo que propició que operaran bajo un programa de "contingencia", que genera un retraso en las transferencias electrónicas.

A finales del mes pasado se afectó el cierre de operaciones en el mercado bursátil, ya que los inversionistas se quedaron cortos de dinero en algunas posiciones, riesgo que tendrán que asumir los bancos involucrados si se confirma que no alcanzaron a procesarse.

Según Panda Security, lo anterior pudo ser **un ataque conocido como Negación de servicio** (DDoS, por sus siglas en inglés), obligando a los organismos bancarios a operar en su sistema alterno, manifestando así la lentitud de los pagos el fin de semana.

Según el informe de Accenture y Ponemon Institute "2017 Cost of Cybercrime", esto nos enseña que cada vez se necesita más tiempo para subsanar ciberataques que emplean malware, en especial hablando de **WannaCry y NotPetya** (55 días frente a los 49 de 2016). Precisamente, este tipo de ataques con software malicioso son los más costosos para las empresas.

Los efectos negativos de un ciberataque pueden ser muy variados: **robo de información, crisis de reputación, pérdidas económicas, daños irreparables en los equipos e infraestructura técnica**, etc. Por eso, es conveniente tener en cuenta una serie de medidas que aumenten el nivel de protección de tu empresa y reduzcan al mínimo el posible impacto del cibercrimen.

Prevenir y nunca lamentar

¿Cómo se pueden controlar estos incidentes? **Panda Security** fue el primer fabricante en fusionar dos tecnologías: la seguridad reactiva del antivirus y la tecnología proactiva para brindar alertas ante comportamiento malicioso. La unión de estos dos tipos de seguridad derivó en un agente capaz de monitorizar en tiempo real todo lo que sucede en el equipo del usuario final.

Según el estudio de Accenture sobre el costo del cibercrimen, un mayor entendimiento de las consecuencias de este fenómeno podría ayudar a los ejecutivos a reducir la brecha entre sus propias defensas y la escalada creatividad de los ataques, así como el aumento en la cantidad de actores amenazantes.

De acuerdo con cifras de diversos actores en la industria de ciberseguridad, durante 2017, se causaron **7.5 millones de ataques de negación de servicio distribuido**, provocando en 56% de los afectados un impacto financiero de entre 10 mil y 100 mil dólares, casi el doble con respecto a los costos relacionados con este tipo de ataques en 2016.

Particularmente **México sufrió 14 mil 237 ataques DDoS,** lo que representó 39 amenazas por día y dos por hora; el tamaño de ataque más grande fue de 44.4 Gbps. El 44.61% de estos ataques provienen desde nuestro mismo país, siguiéndole Estados Unidos (26.96%), Irlanda (16.18%) y Alemania (12.26%).

Más allá de la prevención y remedio, **si falla la seguridad, las empresas se enfrentan a costos inesperados** por no ser capaces de administrar sus negocios de manera eficiente para competir en la economía digital. De ahí que los especialistas recomienden mejorar la seguridad informática de las empresas e instituciones de gobierno.