Principales Ciber-Amenazas para el 2017

Punto de Vista RISCCO - Marzo 2017

RESUMEN EJECUTIVO

En este artículo hemos resumido algunos de los principales ataques cibernéticos ocurridos en el año 2016; ejemplos de costos del cibercrimen; tipos de amenazas que se pronostican para 2017 y algunos consejos de seguridad para ayudar a incrementar la conciencia requerida para afrontar los crecientes, innovadores y desiguales ataques perpetrados por organizaciones que colaboran entre ellos, que se apoyan en arsenales de herramientas, sin limitaciones de horarios laborales o de fronteras geográficas.

© 2009 – 2017 RISCCO. Todos los derechos reservados.

Algunos de los ciberataques de gran impacto durante el año 2016 incluyen:

- Robo de 81 millón de dólares al Banco de Bangladesh por medio de SWIFT, mientras que el objetivo era robar cerca de mil millones de dólares. Con el mismo esquema robaron 12 millones al Banco del Austro en Ecuador y un intento al Tien Phong Bank de Vietnam por 1.3 millones, que fue frustrado.

- Guccifer 2.0 publicó números de celulares, correos y otros datos privados de 193 políticos y de donantes del Partido Demócrata de Estados Unidos.

- El investigador Crhis Vickery encontró datos privados de 87 millones de votantes de México, pocos meses después de un hallazgo similar de 191 millón de votantes de EUA, usando shodan.

- Un grupo de hackers robó de más de 65 millones de dólares en bitcoins a través de la plataforma de intercambio denominada BitFinex.

© 2009 - 2017 RISCCO. Todos los derechos reservados.

- Yahoo reconoció 2 robos de 500 y 1,000 millones de cuentas respectivamente, superando los 167 millones de credenciales robadas a Linkedin en 2012 y los 427 millones robadas a Myspace en 2013.

- FBI, Europol, Eurojust, Interpol y otros asociados lograron desmantelar la red avalancha e incautar 39 servidores utilizados para distribuir malware, spam y phishing en 180 países desde el 2009.

- El ataque más grande de negación de servicios de los últimos 10 años, fue realizado por los New World Hackers que atacaron a DYN (un proveedor de DNS) con la Botnet de IoT Mirai, interrumpiendo servicios de empresas como Twitter, Netflix, Spotify, CNN, PayPal y muchas más.

Estos ejemplos ayudan a entender que el cibercrimen es el negocio más atractivo, rentable y de bajo riesgo para las bandas. Las pérdidas anuales por fraude en EUA se estiman en 620 billones de dólares, mientras que Globalcyberalliance.org indica que en el Reino Unido son 34 billones de libras por año.

© 2009 - 2017 RISCCO. Todos los derechos reservados.

¿Cuáles son las amenazas esperadas para 2017?

1. Incremento y sofisticación del Ransomware, para cobrar dinero como rescate por sus datos.
2. Ataques distribuidos de denegación de servicios (DDoS). Se espera que botnets como Rammit, Mirai, Dorkbot, entre otras, logren mayores ataques de negación de servicios basados en IoT.
3. Tecnologías como criptografía, inteligencia sobre amenazas (threat intelligence) y https, serán utilizadas estratégicamente por los atacantes para violar los esquemas de seguridad.
4. La publicidad engañosa (maladvertising) seguirá su incremento para atraer más víctimas.
5. "Spear-phishing" más inteligente y más realista, menos sospechoso y más difícil de detectar.
6. El Cibercrimen se enfocará en las PYME's. Ataques como los de SWIFT han demostrado que las organizaciones medianas tienen menos recursos para establecer mecanismos de ciberdefensa.
7. Los datos privados y las cuentas privilegiadas que son robadas se venden en la "deep web", muchas veces sin que las víctimas tengan conocimiento de que han sido atacadas.

© 2009 - 2017 RISCCO. Todos los derechos reservados.

¿Qué podemos hacer frente a estas amenazas?

Como parte de las medidas que debe considerar en su programa de ciberseguridad para el 2017, sugerimos las siguientes:

1. Implementar seguridad integrada, en lugar de seguridad por capas.
2. Implementar soluciones de "end point" de última generación.
3. Priorizar los mecanismos de seguridad en función del riesgo.
4. Automatizar tareas de seguridad rutinaria que permita al personal enfocarse en estrategias avanzadas de prevención, detección, reacción, recuperación e investigación de ciberataques.
5. Automatizar los programas de concienciación de ciberseguridad basados en ataques reales.
6. Implementar mecanismos de defensa coordinada. Asegúrese que su equipo de colaboradores hablan el mismo idioma y que están comprometidos con la seguridad de la organización.
7. Asegúrese de tener inventarios automatizados de todos los dispositivos y software autorizado y no autorizado, con configuraciones seguras, que le permitan generar alertas al detectar cambios.

© 2009 - 2017 RISCCO. Todos los derechos reservados.

CONTACTOS

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Raúl Lezcano
t: 279-1410 Ext. 108
rlezcano@riscco.com

riscco.com

Es una compañía panameña, independiente y dedicada, de manera exclusiva, a la consultoría en riesgo tecnológico, seguridad de información y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con ocho (8) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.

© 2009 – 2017 RISCCO. Todos los derechos reservados.