Anuncios

IBM X-Force C-TOC, el primer camión “antihacking” o centro de operaciones tácticas cibernéticas

Madrid - 28 feb 2019: Uno de los objetivos de IBM es mejorar la ciberseguridad, la capacitación y la preparación de las organizaciones en todo el mundo frente a las amenazas de los ciberdelincuentes. Por esta razón, IBM ha desarrollado el primer “camión antihacking” – o centro de operaciones tácticas cibernéticas sobre ruedas X-Force (C-TOC por sus siglas en inglés).

Siguiendo el modelo de los centros de operaciones tácticas de los militares, C-TOC es un puesto de vigilancia de seguridad y un centro de datos completamente operativo, construido dentro de un camión de 18 ruedas. C-TOC está diseñado para sumergir a las empresas en una experiencia que simula un ataque cibernético de una forma totalmente realista, con el objetivo de ayudarles y concienciarles sobre la necesidad de practicar y mejorar su respuesta ante una crisis de este tipo. También se puede configurar como un centro de operaciones para ayudar a empresas y organizaciones a gestionar la ciberseguridad en grandes eventos. Además, puede utilizarse para impartir sesiones de formación tanto a empresas como a estudiantes con edad escolar o universitarios.

C-TOC puede instalarse en casi cualquier lugar, ya que cuenta con comunicaciones autosuficientes, por satélite y celulares y está preparado para adaptarse a una variedad de organizaciones que cada vez más demandan ayuda para prepararse ante el número creciente de ataques cibernéticos.

C-TOC viajará a ciudades de toda Europa en 2019 para brindar capacitación, educación y concienciación sobre la necesidad de estar preparados ante incidentes de ciberseguridad. El calendario inicial incluye paradas en el Reino Unido, Irlanda, los Países Bajos, España, Suiza y Francia. Se pueden encontrar detalles adicionales en el siguiente enlace (Nota de prensa)

Ensayando para responder adecuadamente durante un ataque cibernético: por qué IBM construyó el C-TOC

Cuando se trata de la respuesta a incidentes de ciberseguridad, la velocidad lo es todo: los incidentes de ciberseguridad que tardan más de 30 días en contenerse cuestan un millón de dólares más que los que se detienen dentro del periodo de 30 días. (IBM/Ponemon Institute Report)

Se ha demostrado que contar con un equipo especializado y preparado para responder a incidentes es uno de los factores que más reduce el coste derivado de un ciberataque (IBM/Ponemon Institute Report).

A pesar de los beneficios comprobados, menos del 25% de los profesionales encuestados en todo el mundo dice que su compañía tiene un plan coordinado de respuesta a incidentes aplicado en toda la organización. (IBM/Ponemon Cyber Resiliency Study)

Sobre IBM Seguridad

- Los ingresos de IBM Security anuales ascienden a unos 3.000 millones de dólares.

- IBM es el mayor proveedor de tecnologías de seguridad a las empresas.

- IBM Security cuenta con más de 8.000 expertos dedicados a seguridad; 17.500 clientes en más de 130 países y más de 10.000 patentes relacionadas con seguridad.

- IBM Security Services gestiona 70.000 eventos de seguridad al día.

- Desde 2015, IBM Security ha contratado a casi 2.000 expertos adicionales entre desarrolladores, consultores e investigadores.

Más información sobre IBM Security en la sala de prensa, @IBMSecurity en Twitter y en el blog IBM Security Intelligence blog.

Sobre la ciberseguridad y el cibercrimen

El cibercrimen es el crimen organizado del SXXI y representa la mayor amenaza a las empresas de hoy en día. El 80% de los ciberataques parte de bandas y redes muy organizadas que comparten datos, herramientas y experiencia.

El cibercrimen se está sofisticando y cada año crece su impacto en la economía global. En 2014 costó 445.000 millones de dólares, mientras que en 2016 su impacto ha subido a unos 600.000 millones de dólares (1).

Los cibercriminales se han convertido en organizaciones cada vez más sofisticadas y colaborativas entre ellos. Colaboran en la web oscura compartiendo técnica y lanzando ataques desde redes sociales populares o desde el email. Tienen un nivel organizativo y una productividad que podría ser la envidia de muchos negocios. Por ejemplo, ofrecen soporte a su clientela, garantías económicas si sus herramientas de hackeo no resultan eficaces, etc.

Por eso, es fundamental estar siempre un paso por delante de ellos, razón pro la cual IBM tiene investigadores rastreando la web oscura cada día para monitoriar las últimas estrategias de ciberataque.

Los equipos de seguridad de las empresas se enfrentan a una lacra que crece tanto en volumen de ataques como en volumen de datos robados o comprometidos.

A medida que los ataques se incrementan, aumenta como consecuencia la demanda de profesionales especializados y preparados. Una demanda que no está siendo fácil de cubrir. Se estima que el déficit de talento especializado asciende a 2,93 millones de profesionales (2).

La propuesta de IBM para combatir el cibercrimen se centra en tres cuestiones:

- Colaboración: al igual que los hackers colaboran en la web oscura, los chicos buenos -los profesionales del

mundo de la ciberseguridad- deben mejorar sus métodos de colaboración y compartir información acerca de las amenazas que detectan así como de los métodos para detenerlas antes de que se propaguen a gran escala.

- Utilización de tecnologías cognitivas: las herramientas cognitivas incorporan tecnologías de nueva generación con inteligencia artificial ayudan a los equipos de seguridad de las empresas a anticiparse a las amenazas. Watson for Security ha sido entrenado en el lenguaje de la seguridad. Watson ha leído 2 millones de documentos sobre ciberseguridad y ayuda a los profesionales de este campo a acceder a miles de estudios a través de una interfaz de conversación.
- Centrarse en la respuesta: una respuesta lenta a un ataque tiene un impacto enorme en el coste y en la gravedad e intensidad del daño. Por eso, las empresas deberían prestar atención especial y emplear una estrategia de respuesta a incidentes con los equipos y planes preparados para responder eficaz y rápidamente cuando se produce un ataque.

(1) Informe de McAfee

(2) Informe ISC2

Contacto(s)

Patricia Núñez Canal

IBM Comunicación Externa +34 91 3977782 patricia.nunez@es.ibm.com