IBM avisa de los riesgos de hackeo durante el puente de la Constitución

Madrid - 04 dic 2019: En España, el puente de la Constitución es uno de los periodos del año en el que más se viaja -en 2018 la DGT estimó 6 millones de desplazamientos en España-. En Madrid, por ejemplo, este año los hoteles tienen una previsión de ocupación del 90%, según la Asociación Española de Agencias de Viajes, para las noches del 6 y el 7 de diciembre. Durante estos viajes, se incrementa el riesgo de que los ciberdelincuentes roben información personal, de acuerdo con un estudio de IBM X-Force, en el que advierte de que el sector del transporte se ha convertido en un negocio muy lucrativo para los cibercriminales. Según el índice de amenazas cibernéticas realizado por IBM X-Force en 2019, los viajes y el transporte han sido la segunda industria más atacada, por detrás del sector financiero, mientras que en 2017 eran la décima.

El cibercrimen es el crimen organizado del SXXI y representa una enorme amenaza a las empresas y usuarios de hoy en día. El 80% de los ciberataques parte de bandas y redes muy organizadas que comparten datos, herramientas sofisticadas como Inteligencia Artificial o Cloud y experiencia.

Durante 2018, más de 560 millones de registros se filtraron desde el sector de los viajes y el transporte.

IBM X-Force alerta de que, durante los viajes, los hackers aprovechan para conseguir datos personales procedentes de pasaportes, itinerarios de viaje, sistemas de pago, etc. en un momento en el que, además, los viajeros tienden a relajarse y a optar por la comodidad antes que por la seguridad. De hecho, de acuerdo con una encuesta realizada por Morning Consult y encargada por IBM Seguridad, los turistas y viajeros no son conscientes de los riesgos que se producen durante sus viajes en carretera: solo un 40% de los encuestados creía que durante sus desplazamientos había un mayor riesgo de sufrir un ciberataque y un 70% creó

situaciones de riesgo durante sus viajes en carretera.

"Durante los viajes, las personas somos más vulnerables. Hace cientos de años, los delincuentes eran los piratas. Hoy en día los criminales siguen ahí, aunque con nuevos métodos, muy centrados en el ataque cibernético", afirma Eduardo Argüeso, director de IBM Seguridad en España.

"Cuando las personas estamos en casa, tenemos más control físico y digital de nuestros dispositivos. Sin embargo, cuando viajamos, además de incrementar el número de transacciones que hacemos, transportamos una enorme cantidad de datos personales, lo que nos hace estar mucho más expuestos", añade Eduardo Argüeso.

Sobre la ciberseguridad y el cibercrimen

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, con grandes capacidades tecnológicas como Inteligencia Artificial o Cloud, 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 Inteligencia Articial y la nube: 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.

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

Contacto(s)

Patricia Núñez Canal

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