CONGRESO DE LOS DIPUTADOS
SECRETARÍA GENERAL
REGISTRO GENERAL
15 OCT. 2018 16:00:49
Entrada 106753
SECRETARÍA DE ESTADO DE RELACIONES CON LAS CORTES

RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/37078 a 184/37080 **28/08/2018** **99212 a 99214**
184/37082 **99216**

AUTOR/A: OLANO VELA, Jaime Eduardo de (GP)

RESPUESTA:

En relación con las preguntas de referencia, cabe informar a Su Señoría que el Ciberataque DDoS, del 26 al 28 de agosto, se produjo desde el extranjero y desde el territorio español, siendo en volumen el tráfico ilegitimo procedente de España aproximadamente el 10 % del total. Este porcentaje es similar al de otros ataques recibidos por la web del Banco de España.

No hay evidencia alguna de que los hackers hayan tenido acceso a información sensible ni filtraciones de datos confidenciales.

Los ataques más frecuentes que sufren las entidades financieras en España son los de denegación de servicio, con distintas características técnicas y niveles de intensidad. De hecho, estos ataques ocurren a diario.

Las motivaciones para este tipo de ataques son muy diferentes: pueden estar orquestados por grupos que buscan repercusión mediática para reivindicar sus ideas (los llamados "hacktivistas" como Anonymous), por individuos que quieren dañar a la institución atacada o por delincuentes profesionales con una motivación económica. Estos últimos pueden utilizar la denegación de servicio como una maniobra de distracción mientras llevan a cabo otros ataques que buscan robar información o directamente robar dinero. También es frecuente la exigencia de un rescate económico a cambio de detener el ataque de denegación de servicio.

En todos los casos el principal riesgo al que se enfrentan las entidades atacadas es el riesgo reputacional además del riesgo operacional generado por la no disponibilidad de los servicios ofrecidos por las páginas atacadas. En función de los objetivos y consecuencias del ataque puede haber otros riesgos adicionales, como por ejemplo riesgo legal en caso de reclamaciones de clientes o riesgo de confidencialidad si se produce un acceso no autorizado a información no pública de la entidad o sus clientes. Todo ello generará unos costes económicos que habrá que sumar a los dedicados a la prevención, detección y respuesta frente a este tipo de ataques.

La ciber-seguridad es un área de preocupación creciente para las autoridades supervisoras de todo el mundo. Con el objetivo de mejorar la resistencia del sector financiero europeo ante ciber-ataques el Banco Central Europeo ha publicado en 2018 dos informes "Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures" (expectativas supervisoras) y "TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming" (marco de pruebas avanzadas de ciber-seguridad).

El Banco de España ha puesto en marcha un nuevo sistema que amplía las medidas de mitigación preexistentes y permite una mejor defensa frente a ataques como el sufrido el 26 de agosto.

Madrid, 15 de octubre de 2018

CONGRESO DE LOS DIPUTADOS
SECRETARÍA GENERAL
REGISTRO GENERAL
15 OCT. 2018 16:00:49
Entrada 106753