

ICANN reporta ciberataques a la infraestructura global de Internet

El Ciudadano · 22 de febrero de 2019

El organismo asegura que su trabajo es garantizar la seguridad, la estabilidad y la capacidad de recuperación de los sistemas de identificación global de Internet



La Corporación de Internet para la Asignación de Nombres y Números (en inglés: *Internet Corporation for Assigned Names and Numbers*, ICANN), **reportó que ciberataques masivos en curso atentan contra la infraestructura del Sistema de Nombres de Dominio (DNS)**.

A través de un [comunicado](#) publicado este jueves, el organismo afirma que **está enfocado en garantizar un Internet global estable, seguro y unificado**, pero advirtió del riesgo continuo y significativo que los ataques revisten para esta infraestructura.

En la misiva, ICANN señala el **aumento de los informes de actividades maliciosas dirigidas a la infraestructura de DNS**, por lo que pide “la implementación completa de las Extensiones de seguridad del sistema de nombres de dominio (DNSSEC) en todos los nombres de dominio no seguros”.

En tal sentido, asegura que **su trabajo es garantizar la seguridad, la estabilidad y la capacidad de recuperación de los sistemas** de identificación global de Internet.

El 15 de febrero de 2019, ofreció una lista de verificación de las **precauciones de seguridad recomendadas para los miembros de la industria de nombres de dominio**, registros, registradores, revendedores y otros relacionados, para que tomen la protección de manera proactiva en sus sistemas, los sistemas de sus clientes y la información accesible a través del DNS.

Como explican, **los ataques tienen como objetivo el DNS** y “hay un patrón de ataques multifacéticos que utilizan diferentes metodologías”.

A través de estos ataques **se realizan cambios no autorizados a la estructura de delegación de nombres de dominio**, reemplazando las direcciones de los servidores previstos por direcciones de máquinas controladas por los atacantes.

Esto solo ocurre cuando el DNSSEC, esa tecnología desarrollada para protegerse contra tales cambios al «firmar» datos digitalmente para asegurar su validez, no funciona.

En este contexto, **ICANN toma cartas en el asunto y “exige una implementación completa de la tecnología en todos los dominios”**, a fin de asegurar que los usuarios de Internet alcancen el destino en línea deseado y ayudando a prevenir los llamados ataques «hombre en el medio», en los que un usuario, sin saberlo, es redirigido a un potencial malicioso.

El ente exhortó además a las partes involucradas a producir mejores herramientas y políticas para asegurar el DNS y otras operaciones críticas de Internet.

Por tanto, **ICANN planifica un evento para que la comunidad de Internet aborde la protección del DNS**: la primera es una sesión abierta durante la próxima reunión pública de la ICANN64, del 9 al 14 de marzo de 2019, en Kobe, Japón.

El Comité anfitrión local de ICANN64 (LHC) está constituido por registros y registradores de nombres de dominio, así como por empresas y asociaciones de la industria de las TIC en Japón.

Además, el Ministerio de Asuntos Internos y Comunicaciones actúa como observador en el comité y brinda un apoyo total para que la [reunión de ICANN64 Kobe](#) sea un éxito.

<https://www.elciudadano.cl/rusia/fuerzas-armadas-rusas-toman-medidas-contra-ciberataques/11/14/>

<https://www.elciudadano.cl/economia/mexico-en-alerta-roja-financiera-por-ciberataque/10/24/>

