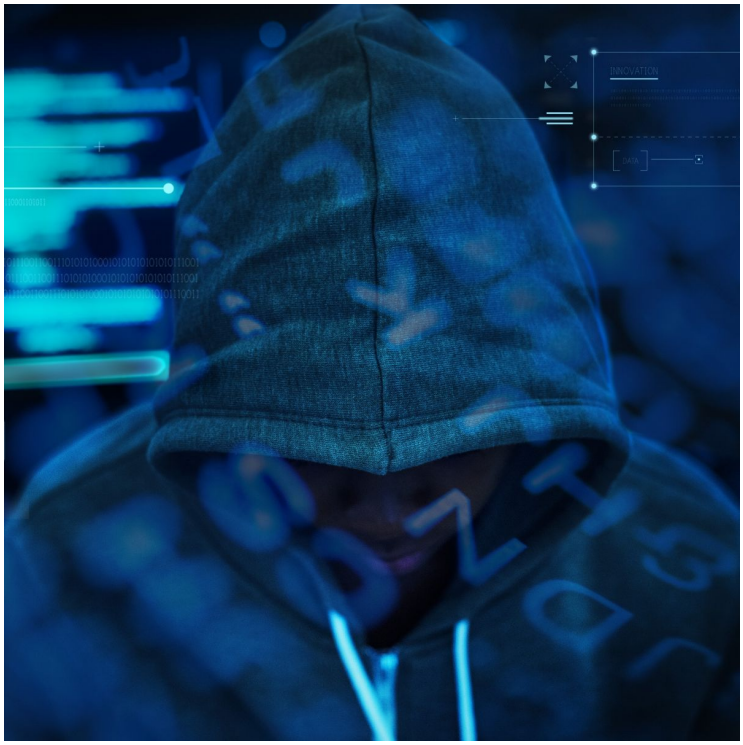
15/12/2024

El ’hackeo’ masivo a la CNMC en España: filtran 2.000 millones de datos de usuarios de telefonía móvil

La Audiencia Nacional ha abierto una investigación por un ciberataque masivo a la Comisión Nacional de los Mercados y la Competencia (CNMC) que expuso 2.000 millones de registros de titulares de telefonía móvil.



Los **ciberataques a organismos públicos** han aumentado en frecuencia e intensidad en los últimos años en España. Las instituciones gubernamentales se han convertido en un objetivo prioritario para los ciberdelincuentes debido a la gran cantidad de datos sensibles que gestionan. Estos ataques no solo exponen la privacidad de millones de ciudadanos, sino que también **comprometen la seguridad nacional**.

Un ejemplo reciente fue el supuesto ataque a la Agencia Tributaria en España, que generó alarma por la **posible filtración de información confidencial de miles de contribuyentes**. Aunque posteriormente se aclaró que no afectó a la AT, el incidente evidenció la vulnerabilidad de las instituciones públicas ante las ciberamenazas.

Ahora, la Comisión Nacional de los Mercados y la Competencia (CNMC) ha sufrido un ciberataque de gran envergadura. La Audiencia Nacional ha asumido la investigación del caso, tras la **filtración de más de 2.000 millones de registros vinculados a usuarios de telefonía móvil**.

La gravedad del ataque, que afectó a 240 GB de datos personales, ha llevado a la jueza María Tardón a clasificarlo como **un delito contra la seguridad nacional**, al considerar a la CNMC un “alto organismo de la Nación”.

Cómo se ha producido el ciberataque a la CNMC?

Al tratarse de **información clasificada como “confidencial”**, el auto sobre el ataque a la CNMC no detalla la fecha en que se produjo. Lo que se sabe es que se produjo una entrada ilícita que ha permitido a los ciberdelincuentes acceder ilegalmente a los sistemas del organismo, extrayendo un gran volumen de información sensible.

La filtración de 2.000 millones de registros sugiere que se trató de una operación bien planificada y posiblemente prolongada en el tiempo.

¿Qué tipo de datos se podrían haber filtrado con el ciberataque a la CNMC?

Los atacantes lograron obtener **240 GB de datos personales relacionados con titulares de líneas de telefonía móvil** .

Este tipo de información podría incluir **nombres, números de teléfono** e información adicional vinculada a los usuarios.

Los expertos en ciberseguridad advierten que esta información podría ser vendida en la dark web o **utilizada en ataques de ingeniería social**, una técnica común para cometer fraudes y suplantaciones de identidad.

¿Cómo van a actuar ante esta filtración masiva?

La Audiencia Nacional **continuará investigando** para identificar a los responsables y esclarecer el origen del ataque.

Hasta el momento, **no se ha confirmado si los atacantes pertenecen a un grupo** de ciberdelincuencia organizado o si están respaldados por un Estado. Tampoco se ha revelado si la CNMC recibió algún aviso previo o intento de extorsión antes de la filtración de los datos.

Los expertos han dado la voz de alarma sobre este 'hackeo': " **No se trata de esperar a que algo pase**, sino de tener los sistemas preparados para actuar antes de que ocurra. Un ataque de esta magnitud pone en evidencia las carencias en la gestión proactiva de ciberseguridad", sentencia Sancho Lerena, CEO de la tecnológica española Pandora FMS.

El experto en gestión IT y seguridad subraya que "la transparencia debe ser tan importante como la tecnología".

Un problema creciente en la esfera pública

El ciberataque a la CNMC pone en riesgo la privacidad de millones de ciudadanos . La filtración de datos personales a gran escala abre la puerta a suplantaciones de identidad, fraudes y posibles casos de ciberacoso.

Sin embargo, este ataque no es un hecho aislado. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha advertido del **aumento de los ciberataques contra infraestructuras críticas y organismos gubernamentales** .

Las instituciones públicas, que gestionan grandes volúmenes de datos personales y comerciales, **son un objetivo atractivo para los ciberdelincuentes**. Por ello, se recomienda la implementación de medidas avanzadas de ciberseguridad, como la autenticación multifactor y la detección proactiva de amenazas.

Cabe recordar que grandes empresas del IBEX 35 han sido víctimas de ciberataques en menos de un año, entre ellas Iberdrola, Banco Santander y Telefónica.

Fuente: https://www.20minutos.es/

LINK DE LA NOTICIA