La Administración de Seguridad de Oleoductos y Materiales Peligrosos (PHMSA) del Departamento de Transporte de Estados Unidos, propuso una multa de casi 1 millón de dólares a Colonial Pipeline, por violar las normas de seguridad federales, lo que empeoró el impacto del ataque de ransomware el año pasado.

La multa de $986,400 dólares es el resultado de una inspección realizada por el regulador de los procedimientos de gestión de la sala de control (CRM) del operador del oleoducto desde enero hasta noviembre de 2020.

> La PHMSA dijo que «*una probable falla en la planificación y preparación adecuadas para el cierre manual y el reinicio de su sistema de tuberías contribuyó a los impactos nacionales cuando la tubería permaneció fuera de servicio luego del ataque cibernético de mayo de 2021».*

Colonial Pipeline, operador del oleoducto de combustible más grande de Estados Unidos, se vio obligado a desconectar de forma temporal sus sistemas a raíz de un ataque de ransomware DarkSide a inicios de mayo de 2021, lo que interrumpió el suministro de gas y provocó una declaración de emergencia regional en 17 estados.

El incidente también vio a la compañía desembolsar 4.4 millones de dólares en rescate al sindicato del crimen cibernético para recuperar el acceso a su red informática, aunque el gobierno de Estados Unidos logró recuperar una parte significativa de los fondos digitales pagados.

> *«El cierre del oleoducto afectó la capacidad de numerosas refinerías para mover productos refinados, y la escasez de suministro creó impactos sociales generalizados mucho después del reinicio»,* dijo PHMSA en un Aviso.

> *«El enfoque ad hoc de Colonial Pipeline hacia la consideración de un 'reinicio manual' creó el potencial de mayores riesgos para la integridad del oleoducto, así como demoras en el reinicio, lo que exacerbó los problemas de suministro y los impactos sociales».*

Actualización: *«Este aviso es el primer paso en un proceso regulatorio de varios pasos y esperamos comprometernos con PHMSA para resolver estos asuntos. Nuestra estructura de comando de incidentes facilita un deliberado enfoque al responder a los eventos»*, dijo un portavoz de Colonial Pipeline a The Hacker News.

> *«Como demostró el incidente de ciberseguridad de 2021, el enfoque de Colonial para operar manualmente nos brinda la flexibilidad y la estructura necesarias para garantizar operaciones seguras continuas a medida que nos adaptamos a eventos no planificados».*

> *«Nuestra coordinación con las partes interesadas del gobierno fue oportuna, eficiente y efectiva, como lo demuestra nuestra capacidad para reiniciar rápidamente la tubería de manera segura cinco días después de que fuimos atacados, lo que siguió a las operaciones manuales localizadas realizadas antes del reinicio oficial».*