CIBERSEGURIDAD, CAMIONES, CARRETERAS, LOGÍSTICA E INFRAESTRUCTURA CRÍTICA
– REPORTE 2 –

Situación general internacional

La interconexión vital entre la ciberseguridad, la infraestructura crítica y el transporte de mercancías ha evolucionado de una conveniencia a una necesidad en la sociedad moderna. Este tejido de conexiones no solo impulsa el comercio y la prosperidad, sino que también presenta desafíos significativos en términos de seguridad y resiliencia.

La Importancia de la Ciberseguridad en la Infraestructura Crítica
La infraestructura crítica, que abarca sistemas de energía, agua, transporte, salud y finanzas, está cada vez más digitalizada. Esta dependencia tecnológica ha aumentado la vulnerabilidad a los ciberataques. Según la Encuesta Global de Seguridad de la Información de PwC de 2022, el 52% de las organizaciones experimentaron un aumento en incidentes de ciberseguridad en comparación con el año anterior.[1] Asimismo, la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) de EE.UU. informó un aumento del 92% en el número de ciber-incidentes reportados en sistemas críticos en 2023, destacando la creciente amenaza que enfrentan estas infraestructuras.[2]

Los ciberataques a la infraestructura crítica pueden tener consecuencias devastadoras. Por ejemplo, un ataque exitoso a una central eléctrica podría causar apagones masivos y paralizar sectores enteros de la economía. De hecho, el informe del Foro Económico Mundial sobre riesgos globales identifica los ciberataques como una de las principales amenazas para la estabilidad económica mundial.[3]

La Conexión Crítica: Infraestructura y Transporte de Mercancías Terrestre
El transporte por carretera desempeña un papel fundamental en la logística global, representando aproximadamente el 80% del transporte de mercancías a nivel mundial.[4] Este sector actúa como un nodo vital en la cadena de suministro, conectando los puertos marítimos y los puntos de origen o destino final de las mercancías. Gracias a su flexibilidad y alcance, el transporte por carretera facilita

[1] 2022 Global Digital Trust Insights Survey, PWC, 2022.
[2] Critical Infrastructure Security and Resilience, Cybersecurity & Infrastructure Security Agency (CISA), 2023.
[3] The Global Risks Report 2023 18th Edition, World Economic Forum, 2023.
[4] Fuentes obtenidas de Organización Mundial del Comercio (OMC) y Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), 2023.

el movimiento eficiente de bienes a través de redes de distribución extensas, lo que contribuye de manera significativa al comercio internacional y al funcionamiento fluido de la economía global.

La interconexión entre la infraestructura crítica y el transporte terrestre es evidente en varios aspectos. Las carreteras y vías férreas forman la columna vertebral de la logística de transporte, permitiendo el movimiento eficiente de bienes. Además, los sistemas de gestión del tráfico y las infraestructuras digitales, como los sistemas de seguimiento de flotas, son cruciales para la eficiencia y seguridad del transporte terrestre de mercancías. Sin embargo, esta interconexión también aumenta la vulnerabilidad a los ciberataques. Un estudio de Symantec encontró que el sector del transporte y la logística fue uno de los más afectados por los ciberataques en 2020, representando el 13% de todas las violaciones de datos.[5] Los ciberataques al transporte terrestre de mercancías pueden tener consecuencias devastadoras, como la paralización del flujo de mercancías en importantes corredores de transporte.

Conclusión

La interdependencia entre la ciberseguridad, la infraestructura crítica y el transporte de mercancías es crucial para el funcionamiento eficiente de la economía global. Salvaguardar esta compleja red esencial se vuelve imperativo para asegurar la continuidad de las operaciones comerciales y preservar la seguridad nacional en un entorno mundial cada vez más interconectado y digitalizado.

Ejemplos internacionales de ataques cibernéticos de gran envergadura

- El 12 de mayo de 2017, hubo un ciberataque masivo que afectó a cientos de miles de computadoras en más de 150 países.[6] Este ataque utilizó un tipo de ransomware[7] llamado WannaCry, que se propagó rápidamente explotando una vulnerabilidad en los sistemas operativos Windows. El ransomware cifraba los archivos de las computadoras infectadas y exigía un rescate en criptomonedas para desbloquearlos. Este ataque afectó a empresas, organizaciones gubernamentales, hospitales y usuarios

[5] Security Summary, Symantec, 2020.

[6] What We Know and Don't Know About the International Cyberattack, The New York Times, 2017.

[7] Ransomware es un tipo de software malicioso que bloquea el acceso a un dispositivo o cifra archivos en él, impidiendo que el usuario pueda utilizarlos. Después de bloquear los archivos, muestra un mensaje solicitando un pago, usualmente en moneda digital, a cambio de desbloquearlos. Estos programas suelen propagarse a través de correos electrónicos fraudulentos, descargas de archivos infectados o aprovechando vulnerabilidades en sistemas no actualizados.

individuales en todo el mundo, causando interrupciones significativas y generando preocupación sobre la seguridad cibernética a nivel global.[8]

- En mayo de 2021, el Colonial Pipeline, uno de los oleoductos más grandes de Estados Unidos que transporta combustible desde Texas hasta la Costa Este, fue objeto de un ataque de ransomware.[9] Los piratas informáticos bloquearon el acceso a los sistemas informáticos de la empresa y exigieron un rescate. Como resultado, Colonial Pipeline se vio obligado a cerrar temporalmente el oleoducto, lo que provocó interrupciones en el suministro de combustible y aumentos de precios en varias regiones del país.

- En 2017, el puerto de Rotterdam, uno de los puertos más grandes del mundo y un importante centro logístico, fue blanco de un ataque cibernético.[10] Los piratas informáticos utilizaron malware para interrumpir los sistemas de gestión de contenedores del puerto, lo que provocó retrasos en las operaciones de carga y descarga de mercancías. Aunque el puerto pudo recuperarse rápidamente, el incidente resaltó la vulnerabilidad de las infraestructuras portuarias a los ataques cibernéticos.

- En 2015, 2016 y 2017 se llevaron a cabo ataques cibernéticos contra el sistema ferroviario de Ucrania, provocando interrupciones masivas en transporte de mercancías y pasajeros.[11] Los piratas informáticos lograron infiltrarse en el sistema de señalización y control del tráfico ferroviario, lo que resultó en la cancelación de trenes y el caos en las estaciones. Este incidente ilustra cómo los ataques cibernéticos pueden afectar directamente la infraestructura de transporte terrestre y causar disrupciones significativas.

- En 2008, se descubrió que piratas informáticos habían comprometido el sistema de peaje electrónico de la autopista de San Francisco, Estados Unidos, conocido como FasTrak. Los hackers lograron acceder al sistema y manipular datos de cuentas de usuarios, lo que planteó preocupaciones sobre la seguridad de los sistemas de peaje, la vulnerabilidad de datos privados y la posibilidad de interrupciones en el transporte por carretera.

---

[8] Algunas de las empresas e instituciones afectadas fueron: FedEx (EE.UU.), Hitachi (Japón), Ministerios públicos de la Federación Rusa, Gas Natural Fenosa y Telefónica (España), Renault (Francia), Servicio Nacional de Salud (Reino Unido), sistemas de ferrocarriles (Alemania).

[9] The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years, Cybersecurity, and Infrastructure Security Agency (CISA), 2023.

[10] Smart port in Rotterdam confounded by cyber-attack, Dutch News, 2017.

[11] Ukraine power cut 'was cyber-attack', BBC, 2017.

- Desde 2016, los ataques cibernéticos, específicamente del tipo ransomware, han proliferado en las empresas de logística, impactando sus sistemas de gestión de flotas de camiones con mayor frecuencia. Estos piratas informáticos logran infiltrarse en el sistema y bloquear el acceso de los operadores de la empresa, ocasionando demoras en las entregas y pérdidas financieras significativas valuadas en millones de dólares. Este tipo de incidentes ha afectado principalmente a empresas logísticas en Europa, Canadá y Estados Unidos en los últimos años. Asimismo, a mediados de 2020, el FBI alertó sobre los riesgos cada vez mayores de ataques cibernéticos dirigidos a los sistemas de Dispositivos de Registro Electrónico o “Bitácora Electrónica” (ELD)[12] en camiones. Estos ataques podrían llegar incluso a implicar el control remoto del vehículo, representando una amenaza significativa para la seguridad y la integridad de la industria del transporte por carretera.[13]

[12] Por sus siglas en inglés.
[13] Cyber Division, Federal Bureau of Investigation (FBI), 2020.