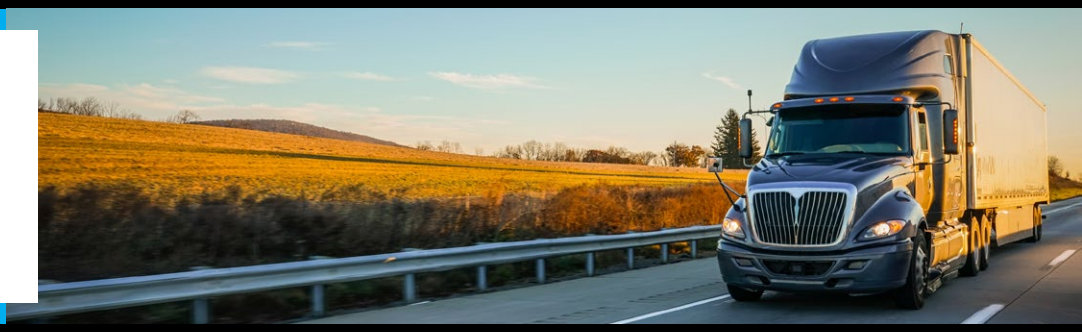
Riesgos cibernéticos en el sector del transporte y logística



Vulnerabilidades a través de la interconectividad

Compañías de transporte y logística dependen en gran medida de la tecnología, debido al rápido avance de la digitalización y la innovación, ahora se encuentran más conectados, eficientes y confiables que nunca, con controles en tiempo real y acceso a la información. Una característica inherente de la conectividad es que las redes de tecnología operativa (TO) y tecnología de la información (TI) a menudo están relacionadas. Con TO proporcionando funcionalidad para dispositivos y procesos de control, y TI proporcionando aplicaciones comerciales y de escritorio, la industria ha avanzado drásticamente.

Nada bueno viene sin un costo y no será una sorpresa que la conectividad también tenga sus inconvenientes, por ejemplo, un problema importante con los sistemas conectados es que las redes de TO a menudo consisten en sistemas más antiguos (heredados) que no tienen parches y están desactualizados. Al conectarse con sistemas de TI más nuevos, este déficit de seguridad puede exponer los puntos débiles de TO. Muchas redes de TO carecen incluso de precauciones simples, como software antivirus, firewalls e inicios de sesión seguros.

En términos generales, cuanto mayor sea el impulso de la digitalización para satisfacer la creciente demanda de velocidad, eficiencia, control y comodidad, mayores serán las vulnerabilidades.

La atracción de los delincuentes cibernéticos

Aparte del legado de los sistemas de TO más antiguos, las empresas de transporte y logística se han convertido en un objetivo principal para los delincuentes cibernéticos por varias razones. Estos incluyen:

- Almacenamiento de datos sensibles y valiosos en línea.
- Uso creciente de dispositivos de Internet de las cosas (IoT/Internet of Things) (por ejemplo, para controlar la temperatura, la vibración, la presión, la humedad). Los dispositivos IoT crean sin duda una superficie de ataque más grande.
  - Una característica notable de los dispositivos IoT es que no siempre incorporan “seguridad por diseño”, lo cual garantiza que los dispositivos sean lo más seguros posible desde el inicio. Parchar los agujeros de seguridad y abordar las vulnerabilidades en los dispositivos IoT es responsabilidad del consumidor, un problema que no siempre es plenamente apreciado por quienes los usan.
- El número de dispositivos móviles conectados de forma remota. Esto aumenta el número de puntos vulnerables del perímetro de la red.
- La creciente amenaza de ataques de phishing contra los empleados.
- Una percepción de que la industria tiene un enfoque en parte reactivo a la seguridad cibernética.
- La creciente sofisticación de los ataques cibernéticos.
- El sector que involucra a proveedores clave de infraestructura crítica. El reciente aumento de los ataques de ransomware contra infraestructuras críticas (especialmente por parte de grupos políticos, estados nacionales o empleados descontentos) significa una mayor exposición, particularmente a las consiguientes pérdidas por interrupción del negocio y la responsabilidad de terceros.

Riesgos adicionales para el sector

Las amenazas adicionales para este sector incluyen ataques que no están dirigidos per se, pero que aún tienen el potencial de ser altamente perjudiciales. Estos incluyen:

- El uso de proveedores de software de terceros. Los recientes ataques cibernéticos a los proveedores de software Accellion, SolarWinds y Kaseya, han hecho hincapié en la posibilidad de daños colaterales a las empresas que utilizan el software. El ataque Not Petya de 2017 involucró un programa maligno (malware) que infectó sistemas informáticos a nivel global, causando efectos duraderos en empresas de todo el mundo. La compañía naviera global Maersk y el conglomerado de transporte FedEx se encontraban entre los afectados; el jefe de cumplimiento de seguridad cibernética de Maersk declaró tiempo después que el ataque sirvió como "una llamada de atención" de que no todos los eventos cibernéticos están dirigidos, y que las organizaciones pueden encontrarse como víctimas no deseadas de estos sucesos.
- El error humano sigue siendo la mayor amenaza de una empresa, y ningún número de firewalls (dispositivos de seguridad de la red que monitorea el tráfico de red) ni aplicaciones de software antivirus mitigará esta exposición.

¿Cuál es el Riesgo Financiero?

Un incidente cibernético en este sector puede conducir a la interrupción o el bloqueo de los procesos, creando daños significativos y consecuencias financieras considerables. Cualquier interrupción en los sistemas que controlan la logística tiene el potencial de paralizar toda la red, siendo el sector del transporte un factor integral en la sociedad y en nuestra vida cotidiana.

Del mismo modo, la compleja interfaz entre las diversas partes del proceso (por ejemplo, embalaje, almacenamiento, entrega y facturación) crea una vulnerabilidad real: cualquier intrusión en esas operaciones puede tener un efecto significativo en los rendimientos financieros de una organización con fuertes pérdidas por interrupción del negocio y costos para responder, remediar y reparar.

Fundamentalmente, los incidentes cibernéticos también pueden afectar a terceros, a los que las organizaciones están obligadas contractualmente a cumplir. Una interrupción para una organización logística puede tener consecuencias importantes debido a que no se cumplen los acuerdos de suministro del cliente, donde la exposición a la responsabilidad con terceros por incumplimiento de contrato es probable. También existe la posibilidad de que el programa maligno (malware) se transmita a terceros a través de un punto débil en el sistema, lo que hace que la red de clientes y contactos de una empresa esté en riesgo, con el potencial de nuevas reclamaciones de responsabilidad.

En resumen, las consecuencias financieras podrían extenderse a:

- Responsabilidad con terceros.
- Exposición regulatoria por violaciones de privacidad.
- Costos de respuesta a incidentes, incluyendo análisis forense de TI, relaciones públicas, gestión de crisis y asesoramiento legal.
- Una demanda de rescate.
- Gastos periféricos de extorsión cibernética.
- Pérdidas de activos digitales.
- Reemplazo de hardware informático que no funciona debido a un evento cibernético.
- Pérdidas por interrupción del negocio.
- Pérdidas por daños a la reputación.

Casos de estudio

- En 2018, una compañía de camiones experimentó un ataque de ransomware que causó caos cuando su flotilla de 300 camiones se vio obligada a paralizarse. La empresa no pudo restablecer su sistema y se vio obligada a pagar un rescate de cinco cifras que sumado a otras pérdidas, incluidas las derivadas de la interrupción del negocio, ascendía a una suma de seis cifras.
- Un ataque cibernético de 2008 en Polonia provocó el caos cuando un joven de 14 años "alteró" un control remoto de TV para cambiar los puntos de vía en el sistema de tranvías de su ciudad. Si bien es una "broma" según su declaración a la policía, el incidente destaca la vulnerabilidad de las redes ferroviarias y la relativa facilidad con la que se llevó a cabo el hackeo.

El Seguro de Cyber

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para todas las empresas dentro del sector del transporte y logística. Reconocer las vulnerabilidades particulares en todo el sector es fundamental, es importante tratar con una firma que tenga experiencia y exposición a los hábitos de compra cibernética de sectores similares. Un corredor/consultor experimentado también puede ayudar con el proceso de identificación y mitigación de riesgos y, cuando corresponda, la transferencia de riesgos por medio de un seguro. El seguro de cyber está diseñado para responder en términos muy amplios, a una violación de seguridad del sistema y una violación de privacidad / datos. Si bien puede haber un grado limitado de concurrencia con otras pólizas, esta concurrencia se está erosionando lentamente a medida que los suscriptores buscan "empujar" las reclamaciones relacionadas con la seguridad cibernética a pólizas de cyber.

A modo de ejemplo, las siguientes pérdidas pueden no ser cubiertas por pólizas más tradicionales:

- Costos de restauración de violación de datos de un ataque cibernético.
- Pérdida reputacional y financiera debido a un ataque cibernético.
- Pérdidas por interrupción del negocio debido a un ataque cibernético.
- Defensa regulatoria, multas y sanciones civiles como resultado de la violación de la privacidad (asegurable por la ley).
- Costos de respuesta a la violación de datos.
- Responsabilidad frente a terceros por determinados eventos cibernéticos.
- Costos de extorsión cibernética.

(Vale la pena señalar que los daños físicos y las lesiones corporales resultantes no suelen estar cubiertos bajo una póliza de cyber independiente, pero las soluciones están disponibles en el mercado).

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector de transporte y logística. Comprender estos riesgos y mitigarlos de manera proactiva es clave.

El equipo de Lockton México trabaja en conjunto con clientes para ayudar a proteger su negocio de los riesgos cibernéticos, desde ransomware hasta phishing, hacks dirigidos, malware, robo de IP y diversas complejidades cibernéticas. Los casos de estudio están inspirados en asuntos reales; sin embargo, algunos hechos pueden haber sido modificados para proteger la confidencialidad del cliente. Estos casos de estudio no constituyen asesoramiento.

Para mayor información:

Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com

Moisés García
ProFin México
moises.garciab@lockton.com