Ataques Cibernéticos en el Sector de Alimentos y Bebidas

El aumento de los ataques cibernéticos contra las empresas de alimentos es quizás un reflejo del hecho de la alta demanda en alimentos. Las amenazas en el sector crean reacciones inmediatas y acaparan la atención de los medios periodísticos. La industria de alimentos y bebidas está a la vanguardia de la tecnología digital e innovación, lo que significa que las empresas dentro del sector son objetivos principales para los atacantes cibernéticos.

Las empresas de alimentos tienen una clasificación baja en términos de inversión en seguridad cibernética e históricamente han mostrado una tendencia a tener menos controles de seguridad básicos y capacidades de gestión de sus activos.

Los principales problemas de seguridad cibernética están relacionados con la violación o pérdida/robo de datos, interrupción del negocio y las pérdidas consecuenciales que pueden ser sustanciales y, en algunos casos devastadoras.

¿Estamos realmente en riesgo?

Es común pensar que los ataques cibernéticos en el contexto de violación de datos, registros de clientes comprometidos y daño a la reputación; todas estas amenazas son reales, por supuesto, pero en el contexto de la industria de alimentos y bebidas, hay otro tipo de amenazas más significantes.

Ransomware es una amenaza cada vez mayor. Un delincuente es capaz de instalar un malware que identifica bases de datos que contienen información confidencial. Esto podría iniciar el proceso de desvío (“secuestro”) de datos confidenciales para su venta y/o distribución.

El delincuente encripta la base de datos o aplicación de la compañía para que se niegue el acceso hasta que la organización pague un rescate a cambio de una clave de descifrado, de lo contrario, los datos se destruyen o se publican. Estos delincuentes cibernéticos pueden ser cualquier persona, desde un empleado descontento, un “hacker” contratado o un activista manifestante de la industria de alimentos.

Si bien la amenaza “estándar” es que difundan los datos confidenciales a menos que se pague el rescate, el sector de alimentos y bebidas es vulnerable a diferentes formas de extorsión.

El sector de alimentos se encuentra en riesgo por la creciente amenaza de “agroterrorismo”; la contaminación intencional del suministro de alimentos para aterrorizar y causar daño. En caso de que el suministro de alimentos se vea comprometido, las organizaciones no tienen más remedio que cerrar sus líneas de producción.

Los delincuentes cibernéticos también están ganando control sobre los sistemas tecnológicos automatizados, amenazando la seguridad de la cadena de alimentos. La prevalencia del internet de las cosas (IoT) y los controladores lógicos programables (PLC) dentro de la refrigeración, el riego y otros procesos, han aumentado el número de vulnerabilidades en una red, comprometiendo en última instancia la seguridad del negocio y, por lo tanto, de los alimentos.

En el caso de una amenaza a la seguridad de los alimentos o la pérdida de control del sistema de la red, el potencial de interrupción del negocio es significativo. El deterioro de los artículos perecederos y el riesgo de retirar los alimentos probablemente causarán pérdidas financieras considerables.

Casos de estudio

Algo para reflexionar

El costo de que pare una sola línea de producción para un fabricante de alimentos y bebidas en el Reino Unido recientemente se estimó una pérdida de £48,000 por hora; £1 millón por día.

Muchas empresas en este sector operan las 24 horas del día, lo que significa que la pérdida de ingresos para una compañía en esta industria es mucho mayor que para una organización que opera durante un horario de oficina estándar; las pérdidas comerciales suelen aumentar rápidamente, lo que tiene el potencial de paralizar la producción y el flujo de efectivo de una empresa.

Un virus desagradable

En abril de 2019, una empresa agroalimentaria francesa se vio afectada por un ataque cibernético que requirió que los sistemas de red se desconectaran para evitar una mayor propagación. La planta cerró durante cinco días, causando una interrupción del negocio significativa generando pérdidas considerables.

Si bien este negocio en particular logró contener el daño en un período de tiempo relativamente corto aunado a que logró mitigar la pérdida a través de su póliza de Cyber, el daño a la confianza del consumidor, la reputación del negocio y su competitividad en el mercado tuvo un impacto negativo en la compañía.

Seguro de Cyber

Se ha opinado que “la industria de alimentos y bebidas es tan susceptible a las amenazas y ataques de seguridad cibernética como cualquier otra industria. La necesidad de asegurar las redes privadas corporativas y la propiedad intelectual está en su punto más alto, al igual que la necesidad de proteger el suministro de alimentos”.[1]

No podemos exagerar la importancia de considerar una estrategia integral de seguridad cibernética para las empresas del sector de alimentos y bebidas. Es vital salvaguardar el sistema de cualquier negocio de alimentos para permitirle proteger sus actividades, productos, clientes, reputación e ingresos.

Es fundamental reconocer las vulnerabilidades particulares en todo el sector de alimentos y bebidas. En Lockton, actuamos para un número significativo de empresas dentro del sector de alimentos y bebidas, lo que nos brinda una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta el sector.

Una póliza de Cyber está diseñada para responder a los siguientes eventos, que no necesariamente serían cumplidos por pólizas más tradicionales:

- Violación de datos de un ataque cibernético.
- Pérdida financiera e impactos reputacionales tanto a la compañía como a los altos directivos por la falla de un sistema informático debido de un ataque malicioso.

- Defensa regulatoria, multas y sanciones civiles como resultado de una violación de la seguridad (asegurable por ley).
- Costos de respuesta a la violación.
- Solicitud de rescate (ransom) tras un ataque a los sistemas informáticos.

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector de alimentos y bebidas. Comprender estos riesgos y mitigarlos de manera proactiva es clave. Nuestro equipo de expertos en riesgos cibernéticos trabajará con usted para crear una solución personalizada que proteja y asegure su negocio exactamente donde lo necesita, asegurando que los riesgos cibernéticos se integren en su proceso de gestión de riesgos.

[1]Cybersecurity in Food, October 22, 2-14 Carrie Straka.

Para mayor información:

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

Moisés García
ProFin México
moises.garciab@lockton.com