Ataques Cibernéticos en el Sector Retail

¿Por qué el sector retail?

El sector de retail está cada vez más conectado, es más eficiente y confiable, con plataformas de ventas y procesos de pago en línea; gracias a la mejora operativa y aplicaciones, el sector ha tenido un incremento drástico y acelerado a raíz de la pandemia y el aumento de las compras en línea. La innovación y digitalización es ahora fundamental en el sector de venta al por menor y aquellas organizaciones que no optan por actualizar sus procesos corren el riesgo de cerrar el negocio.

Dicho esto, la digitalización también tiene sus desventajas; mientras mayor sea el impulso en los sistemas de conexión para cubrir la alta demanda de velocidad, eficiencia, control y practicidad, mayores serán las vulnerabilidades para los delincuentes cibernéticos o para el error humano.

Las empresas minoristas se han convertido en un objetivo principal por varias razones:

- El rápido avance en el comercio electrónico (e-commerce), innovación, y almacenamiento de más datos personales en línea.
- Oportunidades para que los delincuentes cibernéticos provoquen caos financiero, por ejemplo, ataques distribuidos de denegación de servicio, diseñados para saturar la red del destinatario con enormes volúmenes de tráfico en el sistema (deliberadamente programados para coincidir con los períodos con alto flujo de ventas y así aumentar la amenaza).
- Malware: dada su naturaleza tan volátil e innovadora suelen crear nuevas estrategias de ataque, por lo que son una gran amenaza para los sitios de e-commerce.
- Oportunidades para que los delincuentes cibernéticos roben créditos de tiendas, tarjetas de regalo e incentivos que se brindan a los consumidores.
- El uso creciente de dispositivos IoT (Internet of Things) en tiendas físicas (por ejemplo, para controlar la temperatura, la vibración, la humedad) creando una superficie de ataque más grande.
- La creciente amenaza de ataques de phishing contra los empleados.

¿Estamos realmente en riesgo?

Los ataques cibernéticos pueden tomar diversas formas, desde ataques de denegación de servicio, variantes de malware, hasta un click accidental en un enlace de malware incrustado en un correo electrónico de phishing, sin embargo, la amenaza más frecuente es el ransomware.

En los últimos años se ha producido un aumento alarmante en los ataques por ransomware, con una tendencia preocupante; no solo el cifrado del sistema de la compañía y el monto de rescate solicitado, sino que también sustraen información altamente sensible. Normalmente los delincuentes cibernéticos amenazan con publicar la información “secuestrada” a menos que se pague el recate.

Las consecuencias de los ataques cibernéticos variarán según la naturaleza del ataque, pero generalmente implicarán violaciones de privacidad y/o pérdidas por interrupción del negocio.

Exposición de información confidencial

La exposición de información confidencial podría dar lugar a los siguientes costos directos y daños a terceros:

- Daños de terceros asociados con la divulgación inadvertida de información confidencial y personal.
- Gastos de defensa asociados a reclamaciones de terceros.
- Investigación forense de la violación.
- Costos legales, de notificación y de relaciones públicas al tratar la respuesta a la violación.
- Requisitos reglamentarios. Si bien las multas y sanciones solo estarán cubiertas por una póliza de seguro si son asegurables por ley, los costos de responder a una solicitud regulatoria de información generalmente están cubiertos por una póliza de Cyber.
- Daño a la reputación.

Interrupción del negocio

Los resultados de una empresa minorista pueden verse afectados por un ataque cibernético debido a:

- Una página web/aplicación de ventas que no responda y no esté disponible, ocasionaría que los clientes abandonen sus compras en línea representando una pérdida significativa en las ventas.
- Pérdida de clientes a favor de empresas competidoras que no se ven afectadas por el incidente.

Casos de estudio

Un ataque cibernético puede causar daños significativos al sector de retail.

Una consecuencia crítica es la pérdida de control en los sistemas informáticos y los datos de la compañía. Una empresa de ventas en línea experimentó esto recientemente causando un considerable impacto financiero y de reputación.

Se inyectó un script de malware en el sitio web de la empresa a través de una aplicación maliciosa de lenguaje de consulta estructurado (SQL), lo que permitió a los delincuentes cibernéticos acceder a las bases de datos de comercio electrónico, proporcionando acceso a los datos de los clientes.

Al tener conocimiento del ataque, el equipo de seguridad de TI de respuesta al siniestro (designado bajo las disposiciones de la póliza de Cyber) pudo tomar medidas inmediatas para proteger su red y modificar la forma en que se almacenaban sus datos. Desafortunadamente, durante ese proceso se supo que algunos datos de los clientes habían sido comprometidos, incluyendo la filtración de ciertas credenciales. Además de la violación de la privacidad de los datos tuvo el potencial de permitir el robo de saldos de cuentas, créditos, tarjetas de regalo y tarjetas de puntos.

La compañía inmediatamente tomó medidas para notificar a la entidad regulatoria. Con la ayuda de su equipo legal, la empresa notificó a sus clientes de la violación, estableció un call center y contrató a especialistas en relaciones públicas y gestión de crisis para ayudar con la respuesta a los afectados.

En última instancia, se impuso una multa a la compañía por no haber tomado las medidas adecuadas para proteger los datos de sus clientes. Además, recibió una serie de reclamaciones de clientes descontentos con respecto a la divulgación de su información privada.

Los gastos de investigación se cubrieron a través de la póliza de Cyber de la empresa, junto con los gastos de respuesta a la violación (sujeto al pago del deducible). Los costos de responsabilidad por el daño a terceros y de defensa estuvieron dentro de los límites de la póliza. El efecto del ataque, las violaciones de la privacidad y la publicidad resultante han tenido un efecto considerable en la marca y la reputación del minorista. La pérdida de clientes ha sido significativa, lo que ha llevado a una pérdida considerable de ingresos.

Controles de mitigación y seguro específico de Cyber

Es vital proteger los sistemas de una empresa retail lo que servirá para salvaguardar sus actividades, clientes, reputación e ingresos. Reconocer las vulnerabilidades particulares en el sector de retail es fundamental. Un ataque cibernético puede tener ramificaciones de gran alcance. Comprender estos riesgos y mitigarlos de manera proactiva es clave. Un importante proceso de mitigación de riesgos es la transferencia del riesgo a los seguros.

A diferencia de la creencia popular, las pólizas de daños y otras más tradicionales no siempre están diseñadas para responder a un incidente cibernético. De hecho, en los últimos años, las aseguradoras en estas áreas han tomado medidas específicamente para excluir la cobertura relacionada con un ataque cibernético de sus pólizas. El seguro de Cyber es a menudo una mejor opción. Una cobertura afirmativa bajo una póliza de Cyber independiente será vital.

Una parte fundamental de una póliza de protección de datos son los servicios de respuesta a brechas de pérdidas propias y de terceros, con la provisión de asesoramiento forense y legal de TI, así como consultores de relaciones públicas y gestión de crisis para mitigar los daños y garantizar que el negocio vuelva a operar lo antes posible.

Para mayor información:

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

Moisés García
ProFin México
moises.garciab@lockton.com