Ataques Cibernéticos en el Sector Inmobiliario

Hace 5 años los ataques cibernéticos se centraban en los sectores más vulnerables como la salud o los servicios financieros. El sector inmobiliario se ha convertido en un objetivo principal para los atacantes cibernéticos.

¿Estamos realmente en riesgo?

¿Cuánta exposición al riesgo cibernético enfrenta el sector? Transacciones inmobiliarias de alto valor que tienen lugar entre las partes involucradas, realizadas a través de plataformas digitales hacen que la industria sea particularmente vulnerable a los ataques.

Violación de datos

Administradores de propiedades, desarrolladores y empresas de inversión inmobiliaria manejan una gran cantidad de datos confidenciales, incluidas cuentas bancarias, detalles de identificación, detalles de tarjetas de pago, nombres, direcciones y fechas de nacimiento. La responsabilidad ante terceros (el individuo en cuestión o los organismos reguladores de privacidad) debido a una violación de datos, es un riesgo elevado. Además, el daño a la reputación tiene el potencial de crear fuertes implicaciones financieras.

Interconectividad

La tendencia hacia la eficiencia, rentabilidad y fiabilidad en la gestión de bienes inmuebles ha aumentado significativamente la conectividad entre las redes de tecnología y TI. La conexión entre estos sistemas significa que los operadores tienen una supervisión de sus operaciones que no imaginaban hace una década. Un ataque a un sistema de gestión inmobiliaria tiene como consecuencia el acceso a la red informática de una empresa.

Ransomware

El acceso a la red de una compañía conlleva otros riesgos importantes incluidos los ataques de ransomware. En dichos ataques, un delincuente cibernético puede instalar un malware que identifica bases de datos que contienen información confidencial, dando inicio al proceso de desviación de datos confidenciales para su venta y/o distribución en “dark web”; el atacante cifra la base de datos o aplicación del afectado 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 serán destruidos o liberados. En el delicado mundo del sector inmobiliario, la divulgación de datos vulnerables podría tener efectos perjudiciales.

Dispositivos

La prevalencia de dispositivos en el sector (por ejemplo, teléfonos inteligentes y tabletas) y dispositivos IoT (Internet of Things), implica un aumento en los “puntos de contacto” y, por lo tanto, mayor vulnerabilidad. Los atacantes utilizan estos puntos de contacto para infectar un amplio rango de redes, lo que aumenta las amenazas no solo para los datos sino también para los inquilinos (al tomar el control de los sistemas de construcción).

Cadena de suministro

Un proveedor externo, como una aplicación alojada en la nube o una copia de seguridad, pueden ser atacados comprometiendo la información de la compañía. Con la digitalización en línea de los registros de propiedad y las transacciones inmobiliarias, esta dependencia a la cadena de suministro resulta ser un gran problema, cuyas implicaciones se extienden a la interrupción del negocio.

Las pérdidas generadas por interrupción del negocio pueden escalar rápidamente.

Riesgos comerciales

Fuera de los desafíos cibernéticos específicos del sector inmobiliario, existen los riesgos que se observan en todas las organizaciones. Los sistemas de recursos humanos, nómina y pagos, sistemas financieros y corporativos tienen sus propias vulnerabilidades. De hecho, la mayoría de los ataques cibernéticos son contratados para realizar dichos ataques y que exista una remuneración económica, esto se puede vincular al aumento de los ataques relacionados con ransomware y robo de propiedad intelectual.

Casos de estudio

Atacando una ciudad

En mayo de 2019, la ciudad de Baltimore fue golpeada con un ataque de ransomware mediante el cual los delincuentes cibernéticos tomaron el control de los sistemas informáticos de la ciudad. Ocasionando que el mercado de transacciones inmobiliarias se quedara sin acceso a los registros de las propiedades.

Tardaron dos semanas en restablecer las alternativas de papeleo a la "vieja escuela", sin embargo, las alternativas manuales no estaban disponibles de inmediato para todos los procesos transaccionales. Tomó algunas semanas el acceso completo para ser reintegrado. Las ventas registradas cayeron más del 18% y los impactos del ataque aún persisten.

Seguro de Cyber

En Lockton, actuamos para un número significativo de empresas locales y globales dentro del sector inmobiliario, desde empresas, hasta asociaciones público-privadas e inversores inmobiliarios de capital privado. Ofrecemos servicios de seguros innovadores y personalizados a un amplio número de clientes dentro del sector. Esto nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta el área.

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su organización. Es vital resguardar los sistemas de una empresa que le permita proteger sus actividades, clientes, reputación e ingresos, donde reconocer las vulnerabilidades particulares es fundamental.

Vale la pena mencionar que muchas pólizas tradicionales no responderán a una violación cibernética. Una cobertura afirmativa bajo una póliza de Cyber es vital.

Una póliza de protección de datos está diseñada para responder a los siguientes eventos, que no necesariamente serían cubiertos 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 inmobiliario. 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. Reconstruir la confianza es vital.

La seguridad de los datos de sus clientes está en sus manos. Coloque la seguridad de su negocio en las nuestras.

Para mayor información:

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

Moisés García
ProFin México
moises.garciab@lockton.com