Ataques cibernéticos en el sector de arquitectura e ingeniería

Dentro de la industria de la construcción, las empresas colaboran en un entorno digital. Muchas partes interesadas del proyecto, incluidos arquitectos e ingenieros, tienen acceso a plataformas de TI compartidas de una manera que es única para la industria de la construcción. Esta dependencia de redes, aplicaciones de software y datos compartidos proporciona a la industria una conectividad totalmente automatizada, lo que permite la comunicación y el acceso a datos compartidos que no eran dimensionados hace una década.

Este incremento en la eficiencia conlleva mayor exposición al riesgo, particularmente en el sector de la construcción. Por un lado, el gran volumen de datos confidenciales compartidos (incluidos presupuestos, información de ofertas, dibujos técnicos, diseño de productos y datos o secretos comerciales) conlleva riesgos de seguridad adicionales.

Otras características de la industria incluyen el uso generalizado de tabletas, teléfonos inteligentes o computadoras portátiles (lo que aumenta la vulnerabilidad del sistema) y la gran dependencia de subcontratistas y mano de obra transitoria, dando como resultado una gran presión en la capacitación constante.

¿Estamos realmente en riesgo?

Exposición de información corporativa confidencial

La exposición de información confidencial podría dar lugar a las siguientes perdidas propias y a terceros:

- Daños asociados con la divulgación involuntaria de secretos comerciales.
- Reclamaciones de clientes y otras personas por el costo de rediseñar o reconstruir instalaciones o sistemas seguros.
- Investigación forense de la violación cibernética.
- Asesoramiento legal y costos de relaciones públicas sobre cómo responder y reaccionar.
- Gastos de defensa asociados a reclamaciones de terceros.
- Sanciones regulatorias como las multas solo estarán cubiertas por una póliza de seguro si son asegurables por ley, sin embargo, los costos de responder a una investigación del organismo regulador generalmente también están cubiertos por una póliza de Cyber “estándar”.

Violación de la seguridad de la red

- Pérdida de ingresos relacionada con la incapacidad de realizar negocios y proporcionar servicios (debido a la interrupción del negocio, problemas de flujo de efectivo, etc.)
- Daños sufridos por terceros que interactúan con el sistema de una empresa.
- Pérdida de confianza por parte de los clientes y posible daño a la reputación.

Modelaje de información para la construcción

Modelaje de información para la construcción (BIM/Building Information Modeling) es un registro central que permite la entrada de varios partes, ya sea que trabajen de forma independiente para consolidar la información (nivel 2) o trabajando en el mismo modelo integrado al mismo tiempo (nivel 3). Debido a la naturaleza compartida del modelaje de la información y las numerosas partes interconectadas, los riesgos de una violación de seguridad de los datos son mucho mayores, particularmente dentro del nivel 3 de BIM.

Las amenazas incluyen ganancias comerciales por medios delictivos mediante la explotación de la propiedad intelectual, el sabotaje del proyecto o el secuestro de información comercialmente sensible para pedir un rescate. Una plataforma BIM alojada en el sector de arquitectos e ingenieros puede tener implicaciones potenciales de responsabilidad derivadas de exposiciones contractuales con terceros.

> “El gran volumen de datos confidenciales compartidos conlleva riesgos de seguridad adicionales”

Cobertura de responsabilidad civil profesional

¿Cómo interactúa una póliza de cyber y complementa el seguro de responsabilidad civil profesional (E&O/PI) de una empresa?

Cobertura bajo una póliza de responsabilidad cvil profesional.

- Una pérdida cibernética, si estuviera cubierta por la póliza de E&O, estaría sujeta al deducible que tendría que desembolsar el mismo asegurado que a menudo es muy alto para las empresas de construcción el cual representaría un gasto elevado.
- Una pérdida cibernética puede erosionar los límites de PI disponibles para las reclamaciones de errores profesionales. Esto afectaría la siniestralidad, indemnización y potencialmente la prima.
- Para activar la cobertura bajo la póliza de PI, es posible que tenga que haber un error u omisión en la realización de servicios profesionales. Sin embargo, una empresa de arquitectura o ingeniería podría ser responsable por las violaciones de datos o seguridad de la red, incluso en ausencia de un error u omisión. Además, el incidente no siempre estará relacionado con la prestación de servicios profesionales.

Cobertura bajo una póliza de Cyber

- Los costos directos (pérdidas propias), como los costos forenses de TI (para determinar el origen, alcance, extensión de la violación y actuar para contenerla), los costos legales y los costos de relaciones públicas generalmente no están cubiertos por una póliza de PI, por otro lado, bajo una póliza de seguro de cyber si se estarían cubriendo. Una de las principales ventajas de una póliza de cyber es el acceso 24/7 a los servicios de respuesta a incidentes cibernéticos. En esas primeras horas después de un incidente, el acceso inmediato al soporte de TI para determinar el alcance, causa o magnitud del evento cibernético será vital para minimizar el tiempo de inactividad y el daño financiero.
- Las empresas en el sector de construcción operan con plazos y fechas de entrega muy ajustados; es crucial que se mitigue la interrupción del negocio y se mantenga la planificación para garantizar un impacto mínimo en los acuerdos contractuales.
- Las pólizas de seguro de cyber a menudo responderán a una violación independientemente que sea conducta ilícita o esté relacionada con los servicios profesionales.

Casos de estudio

Las pérdidas por interrupción del negocio debido a una suspensión del sistema pueden ser considerables; los ataques pueden tener efectos devastadores.

Los riesgos más grandes siguen siendo la pérdida de datos técnicos, incluidos el diseño de productos, especificaciones y propiedad intelectual, así como la pérdida de tiempo que toma recuperar esa información.

Un caso reciente, un alto directivo de una gran empresa de ingeniería civil descargó inadvertidamente un virus de ransomware en una computadora portátil, lo que provocó que el virus se propagara por todo el servidor. Se tardó una semana en restaurar los archivos de copia de seguridad, y durante ese tiempo, la empresa no tuvo acceso a los documentos del servidor. La pérdida fue significativa.

Seguro de Cyber

En Lockton, nos especializamos en programas de seguros grandes y complejos para empresas globales de arquitectura e ingeniería civil. Nuestro programa de seguros se adapta a las necesidades de las empresas, lo que garantiza una cobertura adecuada para todas las partes en todas las líneas de cobertura. Esta experiencia en la industria nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta la industria de la construcción.

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su organización de arquitectura o de ingeniería. Es vital proteger los sistemas de una empresa para permitirle proteger sus actividades, clientes, reputación e ingresos. Reconocer las vulnerabilidades específicas del sector de la construcción es fundamental.

Además, las empresas de arquitectos e ingenieros están encontrando cada vez más seguido el requisito indispensable por solicitud de sus clientes en los contratos de prestación de servicios, contar con algún tipo de seguro de privacidad y protección de datos, dada la alta exposición en esta área.

Un ataque cibernético puede tener ramificaciones de gran alcance. Comprender estos riesgos y mitigarlos de forma 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 necesite y garantice que los riesgos cibernéticos se integran en su proceso de gestión de riesgos.

Mantener la confianza es vital.

La seguridad de sus clientes está en sus manos. Ponga la seguridad de su empresa en las nuestras.

Para mayor información:

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

Moisés García
ProFin México
moises.garciab@lockton.com