Ataques Cibernéticos en el Sector Contable

El sector de la contabilidad se ha convertido en un objetivo principal para los delincuentes cibernéticos, actualmente se ha presentado un incremento en los ataques cibernéticos. Esto se debe a varias razones, particularmente porque los contadores manejan grandes cantidades de información confidencial y sensible de los clientes que tiene un valor considerable para los delincuentes.

Por su propia naturaleza, las firmas de contabilidad manejan información confidencial de sus clientes, incluidos detalles financieros, declaraciones de impuestos, números de identificación, inversiones en activos, estrategias corporativas y propiedad intelectual. Cualquier filtración de esta información, podría causar pérdidas financieras devastadoras y daños a la reputación.

Muchos creen que las amenazas al sector contable se centran en las grandes empresas. Esto quizás se deba al impacto que tienen los noticieros al momento de publicar sus artículos sobre las violaciones de datos contra empresas de alto perfil (por ejemplo, Deloitte y PwC). La impresión de que las empresas más pequeñas no son tan vulnerables está lejos de ser cierta y, de hecho, las empresas de contabilidad tradicionales (en particular las del mercado pequeño y mediano) son vistas como objetivos fáciles.

Las organizaciones más grandes a menudo tienen mayores presupuestos de seguridad y recursos para implementar y/o robustecer la seguridad cibernética, mientras que las empresas más pequeñas pueden no tener los recursos internos para comprometer ese mismo nivel de inversión en seguridad.

No cabe duda de que las firmas de contabilidad se enfrentan al mismo tipo de riesgos cibernéticos que cualquier otra empresa. De igual manera, los contadores tienen un papel importante al momento de asesorar a sus clientes sobre los aspectos estratégicos y operativos de los negocios de sus clientes, lo que requiere mayor comprensión sobre el panorama actual de amenazas cibernéticas.

¿Estamos realmente en riesgo?

PwC estima que el sector financiero tiene más del 30% de probabilidad de ser atacados a comparación de otros sectores y, ciertamente los resultados obtenidos demuestran la veracidad de la estimación.

Los servicios empresariales y profesionales figuran constantemente entre los cinco sectores más atacados. Los ataques de phishing (Intentos fraudulentos de obtener información a través de una forma electrónica de comunicación, mediante la cual el delincuente roba la identidad de un contacto de confianza) son típicos. El delincuente cibernético a menudo utiliza un correo electrónico como un tipo de arma para tratar de obtener información o conseguir que el destinatario haga click en un enlace o descargue un archivo adjunto.

Los riesgos asociados con el uso de tabletas, teléfonos inteligentes y otros dispositivos no pueden exagerarse: mayor acceso y flexibilidad a la red conlleva un riesgo de seguridad alto, desde el robo de datos hasta malware y virus dañinos. Tales amenazas presentan un riesgo considerable que debe ser entendido y mitigado lo antes posible.

Además del impacto financiero, se debe considerar el daño potencial a la reputación. Este sector se basa en la confianza y discreción: en el sector de la contabilidad, la confidencialidad del cliente es un valor fundamental. Mantener una reputación saludable está en el corazón de cualquier firma de contabilidad exitosa, lo cual es una parte fundamental de su estrategia comercial.

La pérdida de datos de los clientes puede tener un impacto devastador en la credibilidad de la empresa y su posición a largo plazo en el mercado. La falta de protección de la información altamente confidencial del cliente puede poner en riesgo a toda la organización.

Casos de estudio

Una reacción en cadena

Un ataque de malware a un proveedor global de software de contabilidad tuvo un impacto negativo en diversas plataformas comerciales. La empresa se vio obligada a desconectar algunas de sus aplicaciones de software basadas en la nube. El servicio a la mayoría de las aplicaciones y plataformas de sus clientes se restableció durante un período de 6 días y se llevó a cabo una investigación completa, los clientes de la empresa fueron sometidos a importantes interrupciones y retrasos, dando como resultado no poder acceder a los datos de sus propios clientes.

Problema fiscal

Un contador de impuestos recibió un correo electrónico aparentemente de un cliente. Lejos de estar lleno con errores ortográficos y otros signos reveladores que podrían indicar que el correo electrónico era fraudulento, el contador fue engañado. A pesar de haber completado la capacitación sobre cómo detectar correos electrónicos de phishing, debido a la sofisticación de esta estafa en particular, el contador no reconoció el "phish" y respondió al correo electrónico.

El delincuente cibernético envió un archivo que supuestamente contenía la información fiscal de un cliente, una vez abierto por el contador, causó que el malware se extendiera por todo el sistema informático, permitiendo al estafador robar información privada, posteriormente, el atacante utilizó la información confidencial para acceder a cuentas bancarias y enviar más correos electrónicos fraudulentos a otros contactos que contenía el directorio del contador.

Valor de la información

La firma global de contabilidad Deloitte sufrió una interrupción significativa a través de un ataque a un correo electrónico, accediendo a datos de 350 clientes; Deloitte ha confirmado que, desde este ataque su protocolo de seguridad ha sido objeto de una revisión exhaustiva, en la que participa un equipo de expertos en seguridad cibernética.

Seguro de Cyber

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética en el sector contable. En Lockton, actuamos para diversas firmas de contabilidad. Esto nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones que enfrenta la industria.

Vale la pena mencionar que muchas pólizas tradicionales pueden no responder a un incidente cibernético, 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 se cumplirían con 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 contabilidad. 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.

Para mayor información:

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

Moisés García
ProFin México
moises.garciab@lockton.com