Ataques Cibernéticos en el Sector Legal

Los despachos de abogados se han vuelto objetivos atractivos para los delincuentes cibernéticos, lo cual está desencadenando un incremento en los ataques al sector; una de las razones principales es el acceso de las empresas a información confidencial y sensible de los clientes, generalmente de gran valor. Por su propia naturaleza, los despachos de abogados a menudo manejan la información privada y comercial más sensible de sus clientes.

¿Por qué el sector de servicios legales?

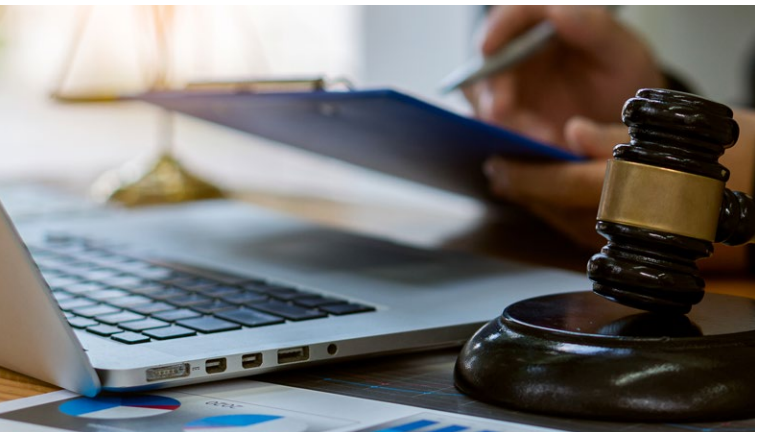
Los despachos de abogados administran grandes cantidades de dinero de los clientes. El "Fraude del viernes por la tarde" es, como su nombre indica, el término utilizado para los ataques cibernéticos (a menudo un viernes por la tarde para que coincida con las transacciones tradicionales y dar al atacante el fin de semana para evitar la detección). Los delincuentes cibernéticos utilizan diversos medios para inducir a los miembros del personal a transferir dinero a su cuenta bancaria, a menudo involucrando alguna forma de interceptación de correo electrónico. El "fraude del viernes por la tarde" representa el 75% de los delitos cibernéticos reportados a la Autoridad de Regulación de Abogados de Reino Unido y Gales.

Tradicionalmente, los despachos de abogados (particularmente aquellos en el mercado pequeño y mediano) son vistos como objetivos fáciles. Las organizaciones más grandes a menudo cuentan con presupuestos amplios de seguridad y recursos para implementar fuertes defensas internas y perimetrales, pero muchos despachos no tienen los recursos internos para comprometer ese mismo nivel de inversión en seguridad de TI, dando como resultado menor seguridad a los eventos cibernéticos. Otros sectores, como la salud y los servicios financieros, generalmente cuentan con seguridad mucho más sofisticada que sus asesores legales.

¿Estamos realmente en riesgo?

La Encuesta Anual de Bufetes de Abogados 2019 realizada por PwC reveló una estadística alarmante: el 100% de las 100 principales empresas sufrieron un evento de seguridad cibernética en los últimos 12 meses, donde los ataques de phishing fueron los más comunes del sector. Phishing es un intento fraudulento de obtener información a través de una forma electrónica de comunicación, mediante la cual el delincuente se "disfraza" (suplanta la identidad) de un contacto confiable. El delincuente generalmente usa un correo electrónico como un tipo de arma para tratar de obtener información o para que el destinatario haga click en un enlace o descargue un archivo adjunto.

DLA Piper, uno de los bufetes de abogados más grandes del mundo, experimentó un evento cibernético que paralizó su actividad en 2017 dejando gravemente afectado a través de un "ransomware" NotPetya. Su red se infectó a través de un proveedor, cifrando todos los archivos afectados. El sistema de seguridad de DLA Piper detectó el malware y el equipo respondió rápidamente para mitigar la emergencia. El sistema fue finalmente recuperado de nuevo en línea, pero no sin enormes ramificaciones financieras, incluido el costo de financiar 15,000 horas extras para los trabajadores de TI.



Si bien la mayoría de los abogados están generalmente familiarizados con este tipo de ataque de ransomware "tradicional", en los últimos meses ha surgido una nueva forma de ransomware, conocida como Maze; es alarmante que este tipo de ataque tenga dos "vertientes", no solo se cifran los datos y se exige un rescate con la garantía de descifrarlos, sino que también se filtran los datos. Por lo general, los delincuentes cibernéticos publican los nombres de las víctimas en el sitio web de Maze con la garantía de que los datos robados de las víctimas se liberarán lentamente si no se paga un segundo rescate. Obviamente, se ejerce mayor presión sobre la empresa por parte de las personas que no quieren que su información confidencial se haga pública.

El sector legal se ha convertido en uno de los principales objetivos de Maze. Somos conscientes de al menos siete bufetes de abogados cuyas redes han sido infectadas recientemente por este ransomware, más comúnmente introducido a través de un archivo adjunto malicioso dentro de un correo electrónico bien redactado, lo que demuestra un gran conocimiento interno sobre el funcionamiento de los bufetes de abogados.

Aparte de la exposición del sector legal a los delincuentes cibernéticos, los bufetes de abogados también son vulnerables a los riesgos asociados con el uso por parte de los colaboradores de tabletas, teléfonos inteligentes y otros dispositivos, ya que, mayor acceso y flexibilidad conlleva un riesgo de seguridad mucho mayor, desde fugas de datos hasta malware y virus dañinos.

Las amenazas cibernéticas presentan un riesgo considerable para el sector legal; además del impacto financiero y el daño a la reputación es enorme. Este sector se basa en la confianza y discreción.

Aquellos que ejercen tienen la confidencialidad del cliente como un valor fundamental. Mantener una buena reputación es el objetivo de cualquier bufete de abogados exitoso y una parte clave de su estrategia comercial. La pérdida de datos de 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 todo el bufete.

Casos de estudio

Eliminación

En un bufete de abogados asegurado, un asociado recibió por correo electrónico un link que lo direccionó a un malware, lo que causó la eliminación de todos los discos duros disponibles para él, y se expandió el incidente hasta llegar a eliminar la propiedad intelectual de la empresa y la información patentada de los dispositivos de almacenamiento y sistemas de respaldo. El equipo de respuesta de seguridad cibernética de la compañía de seguros trabajó estrechamente con el bufete de abogados para recrear todas las aplicaciones e información que se habían borrado, un proceso que tardó aproximadamente 1,100 horas en completarse. El bufete de abogados recibió aproximadamente £ 250,000 en costos.

Seguimiento al hackeo

Un bufete de abogados asegurado recibió una llamada de un contratista de TI que informó que había estado rastreando operaciones de hackeo relacionado con un nombre de dominio en particular. El contratista informó que había detectado pruebas de que las direcciones IP estaban asociadas a los ordenadores del bufete de abogados, supuestamente se comunicaban con el nombre del dominio sospechoso. La firma contrató a un investigador forense para ayudar con la investigación y asesoría legal para brindar asesoramiento respecto a la violación. Estos servicios cuestan entre £ 320,000 y £ 480,000, estaban cubiertos por la póliza de cyber.

Phishing

Aproximadamente 100 abogados y miembros del personal fueron engañados en un correo electrónico de phishing adjuntando un archivo que parecía ser de trabajo. Cuando cada usuario intentaba abrir los datos adjuntos, se le pedía que escribiera su nombre de usuario y contraseña de Outlook. Durante las siguientes 20 horas, el intruso ingresó al servidor Outlook de la empresa y accedió a varios cientos de mensajes de correos electrónicos. La firma contrató a un consultor forense y un bufete de abogados, el asunto se resolvió dentro de la firma.

Perdidos en el laberinto

El grupo de delincuentes cibernéticos “Maze” secuestraron la red de un bufete estadounidense de 11 abogados. La empresa no pagó el dinero exigido dentro del plazo, lo que provocó la publicación de los datos robados. La información publicada en el sitio web de Maze incluía información altamente personal y sensible sobre casos de lesiones personales, acuerdos de honorarios y formularios de consentimiento del paciente. El bufete no ha hecho ningún comentario público al respecto.

El Seguro de Cyber

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su firma de abogados. En Lockton, actualmente representamos a 23 de los 100 principales bufetes de abogados de Inglaterra y Gales. Fuera del Top 100, contamos con una amplia cartera dedicada al sector legal. Esto nos da una excelente exposición a los hábitos de compra cibernética y las exposiciones a las que se enfrenta el sector legal.

Es importante mencionar que muchas pólizas tradicionales no responderán a una violación cibernética. Una cobertura afirmativa bajo una póliza de cyber independiente será vital.

Una póliza de cyber está diseñada para responder a los siguientes eventos, que no necesariamente se cubrirían con pólizas más tradicionales:

- Violación de datos por 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 a un ataque malicioso.
- Defensa regulatoria y cobertura de multas y sanciones como resultado de una violación de seguridad (asegurable por ley).
- Costos de respuesta a la violación.
- Peticiones de rescate tras un ataque a sistemas informáticos.

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector jurídico. Es fundamental comprender los riesgos y mitigarlos de forma proactiva. 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, garantizando que los riesgos cibernéticos se integren en su proceso de gestión de riesgos.

La seguridad de los datos 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