Akamai

WHITE PAPER

Protección de los bufetes de abogados modernos

Protección de aplicaciones y datos críticos de los clientes

Introducción

Los profesionales del sector jurídico manejan datos confidenciales cada día. Con eso en mente, muchas empresas están invirtiendo en controles de seguridad más avanzados y centrando sus esfuerzos en diseñar sus sistemas y procesos de TI en torno al concepto de Zero Trust, para proteger sus aplicaciones críticas y controlar el acceso de los usuarios finales.

El enfoque Zero Trust implementa un modelo de privilegios mínimos, lo que garantiza que los usuarios, sistemas y aplicaciones autorizados solo tengan el acceso adecuado según sus respectivas funciones, a la vez que protege contra el movimiento lateral, el ransomware y el acceso no autorizado. Una de las formas más flexibles y seguras de implementar el enfoque Zero Trust es utilizar la microsegmentación.

Para entender la importancia de todo esto, repasemos un poco la historia.

Filtraciones de gran repercusión: una llamada de atención al sector jurídico

Durante años, las autoridades federales estadounidenses han alertado de que los grandes bufetes de abogados son objetivos fáciles para los ciberdelincuentes, ya que albergan repositorios de datos corporativos con información detallada. Ya en 2009, el FBI comenzó a advertir a los principales bufetes de abogados de que estaban en el punto de mira de ciberdelincuentes organizados. En 2011, llegaron a invitar a 200 de los mayores bufetes de abogados para abordar el aumento de ciberataques sofisticados dirigidos al sector.

> **Una de las formas más flexibles y seguras de implementar el enfoque Zero Trust es utilizar la microsegmentación.**

Desde 2014, más de 100 bufetes de abogados en 14 estados han informado de filtraciones de datos, según Law.com. El informe Legal Technology Survey Report de 2022 del Colegio de Abogados de Estados Unidos (ABA), una encuesta anual que explora el uso de la tecnología en el sector jurídico, reveló que más de una cuarta parte de los bufetes de abogados (de todos los tamaños) había sufrido una filtración. El impacto de las filtraciones abarca desde tiempo de inactividad, causado por el ransomware, hasta largas disputas legales cuando los datos de los clientes aparezcan en Internet.

En 2015, el sector jurídico apareció por primera vez en la clasificación anual de Cisco de sectores objetivo de los hackers. Como consecuencia, muchas instituciones financieras han comenzado a exigir a los bufetes de abogados que se sometan a auditorías periódicas de sus prácticas de ciberseguridad para hacer negocios con ellos.

En particular, dos filtraciones masivas de los bufetes de abogados internacionales Mossack Fonseca & Co y DLA Piper sirvieron como una llamada de atención a todo el sector jurídico y financiero. En la filtración conocida como los "Papeles de Panamá", se filtraron más de 11 millones de documentos, equivalentes a más de cuatro décadas de registros, del bufete de abogados Mossack Fonseca & Co. La filtración expuso paraísos fiscales y las cuentas extraterritoriales de empresas globales y líderes mundiales influyentes, lo que tuvo graves consecuencias. En 2018, la empresa anunció su cierre, debido en gran medida a las consecuencias de la filtración. Los bufetes de abogados tienen la responsabilidad ética y fiduciaria de hacer todos los esfuerzos razonables para proteger la información que poseen. La filtración de datos de los "Papeles de Panamá" representa la mayor brecha de confidencialidad hasta ahora entre un bufete de abogados y sus clientes, y ha contribuido a que tenga lugar un cambio en cómo enfoca la ciberseguridad este sector. Sin embargo, a pesar del nuevo enfoque centrado en mejorar la estrategia de seguridad, los atacantes muestran pocas señales de ralentización.

> **Más de 1 de cada 4 bufetes de abogados ha sufrido una filtración.**
>
> **— Informe Legal Technology Survey Report de 2022 del Colegio de Abogados de Estados Unidos**

Casi al mismo tiempo que la filtración de Mossack Fonseca & Co., DLA Piper, uno de los bufetes de abogados más destacados del mundo con presencia en más de 40 países, fue víctima de un ataque de malware NotPetya. Esto le costó a la empresa semanas de interrupciones, millones en pérdidas de volumen de negocio, costes de recuperación y una publicidad nefasta.

Más recientemente, después de un ataque de ransomware, Grubman Shire Meiselas & Sacks perdió 756 GB de datos sobre su clientela de alto perfil, como Lady Gaga, LeBron James y Madonna. El bufete de abogados se mostró reacio a pagar el rescate, por lo que los atacantes filtraron información sobre Lady Gaga y subastaron lo que afirmaron que eran datos que contenían detalles sobre otros clientes.

Bufetes de abogados modernos: ha llegado la hora de adoptar soluciones de ciberseguridad modernas

La mayoría de las filtraciones descritas han implicado ataques mediante amenazas persistentes avanzadas (APT), que incluyen phishing, malware y ransomware, para robar datos confidenciales de clientes, materiales sobre fusiones, propiedad intelectual e información financiera. Atraídos por ingentes cantidades de dinero, los atacantes cuentan con un apoyo cada vez mayor por parte de grupos de delincuencia organizada que realizan inversiones significativas en herramientas de ataque y equipos profesionales.

> **Las empresas que carecen de una segmentación adecuada en su entorno de TI corren el riesgo de que se les deniegue la cobertura en caso de filtración de datos.**

Hoy en día, cada vez más clientes consideran la ciberseguridad un factor importante a la hora de decidir con qué bufete de abogados hacer negocios. Las empresas que carecen de controles de seguridad modernos son más propensas a perder acuerdos en comparación con las empresas que han tomado medidas para mejorar su estrategia de seguridad y demostrar su compromiso con la protección de los datos de los clientes. Además, muchas aseguradoras cibernéticas exigen ahora algún tipo de segmentación de las aplicaciones y los datos confidenciales. Las empresas que carecen de una segmentación adecuada en su entorno de TI corren el riesgo de que se les deniegue la cobertura en caso de filtración de datos.

La pieza que falta en el puzle: protección de las aplicaciones críticas de la empresa

Como puede ver, los bufetes de abogados ya no son el repositorio seguro de información privilegiada que solían ser. Hoy en día, los ciberdelincuentes reconocen a los bufetes de abogados como almacenes de datos corporativos confidenciales y únicos que son un objetivo óptimo para los ataques de ciberseguridad.

De hecho, a menudo se considera que los bufetes de abogados son blancos más fáciles que la mayoría de sus clientes. Por eso, un atacante que desee obtener datos específicos de una empresa suele intentar primero obtener esos datos a través de su bufete de abogados. La naturaleza confidencial y la variedad de información que almacenan los bufetes de abogados, junto con sus controles de seguridad generalmente más débiles, hacen que sean un objetivo lucrativo para los atacantes.

Los atacantes están increíblemente interesados en la información almacenada en las aplicaciones esenciales de los bufetes de abogados, en particular en su sistema de gestión de documentos (DMS) y en los correos electrónicos. Desde el punto de vista de la seguridad de TI, las aplicaciones empresariales más importantes de un bufete de abogados son sus aplicaciones de DMS y de correo electrónico. Estas aplicaciones poseen la mayor parte de la información confidencial y privilegiada de los clientes, y en muchos casos ya no residen únicamente en centros de datos locales.

Las aplicaciones de DMS cumplen una amplia gama de funciones, entre las que se incluyen: organización centralizada de archivos y carpetas, gestión de versiones, gestión de correo electrónico, edición de documentos, indexación y búsqueda, gestión de permisos, etc. A menudo se implementan en entornos de TI heterogéneos con una combinación de servidores virtualizados y bare metal, y requieren la integración con otros sistemas con distintos niveles de seguridad interna. Aunque estas integraciones pueden hacer que un DMS sea más útil para un bufete de abogados, también pueden hacerlo menos seguro y aumentar drásticamente su superficie de ataque.

Los terminales también se han vuelto tan móviles y dinámicos que las soluciones de seguridad tradicionales a menudo no pueden protegerlos, ya que, al igual que muchas organizaciones, los bufetes de abogados han centrado principalmente sus inversiones en herramientas de seguridad en el perímetro. Estas soluciones ya no proporcionan el nivel de protección que necesitan los bufetes de abogados para proteger las aplicaciones críticas. Además, lo cierto es que muchos bufetes de abogados siguen careciendo de los controles necesarios para detectar o evitar que un atacante se mueva lateralmente y llegue a sistemas de datos confidenciales una vez que ha logrado acceder a la red a través de un terminal vulnerable.

Teniendo en cuenta todos estos desafíos, muchos bufetes de abogados modernos están empezando a invertir en una nueva generación de soluciones de ciberseguridad capaces de satisfacer sus necesidades únicas y en constante cambio. La segmentación basada en software, y en concreto la microsegmentación, admite un enfoque Zero Trust para proteger las aplicaciones y los datos críticos, ya que proporciona un enfoque más detallado para controlar las comunicaciones dentro de la red, lo que permite que solo los usuarios y sistemas autorizados se comuniquen con las aplicaciones críticas. Esto hace que a los atacantes les cueste mucho más moverse lateralmente por la red, limitando así el alcance de una posible filtración.

La COVID-19 ha hecho que los retos sean todavía más complejos:

- Muchos bufetes de abogados han adoptado un modelo de teletrabajo
- Debido a esto, los empleados ya no están conectados a la red desde su oficina corporativa, sino desde redes domésticas no seguras
- El mayor uso de soluciones de VPN y VDI hizo que la implementación de políticas de seguridad y la asignación del tráfico de red a los usuarios autorizados resultaran aún más difíciles

Cuatro formas en las que Akamai ayuda a los bufetes de abogados a proteger los datos de los clientes

Visibilidad completa

Obtenga una visibilidad completa de las cargas de trabajo para estar al tanto de todas las conexiones abiertas a aplicaciones que contienen datos confidenciales.

Control del acceso de los usuarios

Implemente políticas que controlen el acceso a las aplicaciones y los datos, independientemente de dónde residan: en el entorno local o en la nube.

Segmentación basada en software

Microsegmente de forma rápida y flexible las aplicaciones críticas, como el DMS y el correo electrónico, para limitar la exposición en caso de filtración.

Detección y prevención de amenazas

Combine la segmentación dinámica con funciones de engaño para detectar y contener las filtraciones activas y proteger los datos de los clientes.

Protección unificada con Akamai Guardicore Segmentation

Akamai Guardicore Segmentation ofrece la solución de microsegmentación más completa del sector para proteger las aplicaciones esenciales. Acelera drásticamente la implementación de políticas de segmentación, simplifica el mantenimiento continuo y, en última instancia, es más eficaz a la hora de mitigar las amenazas que dependen del movimiento lateral para tener éxito.

> **Para proteger mejor los datos de los clientes, muchos bufetes de abogados están recurriendo a soluciones como la microsegmentación para adoptar un enfoque más detallado a la hora de controlar las comunicaciones dentro de la red, lo que permite que solo los usuarios y sistemas autorizados se comuniquen con las aplicaciones críticas.**

Nuestra solución proporciona un mapa visual de todas las aplicaciones y otros activos de su centro de datos, junto con sus dependencias. Entonces, los operadores de seguridad pueden crear y aplicar de forma rápida e intuitiva políticas de seguridad a nivel de proceso y red para aislar y segmentar aplicaciones y activos esenciales. Este enfoque de segmentación definido por software no depende de la infraestructura subyacente, lo que permite proteger de forma coherente las cargas de trabajo que abarcan sistemas locales (tanto antiguos como modernos), máquinas virtuales, contenedores, nubes y dispositivos.

Se pueden crear políticas en torno a aplicaciones individuales o agrupadas de manera lógica, independientemente de dónde residan en el centro de datos. Estas políticas dictan qué aplicaciones pueden o no comunicarse entre sí, lo que favorece un enfoque Zero Trust. Otra importante ventaja exclusiva de Akamai Guardicore Segmentation son nuestras funciones integradas de detección y respuesta a filtraciones de datos, las cuales hacen que sea más sencillo gestionar varias herramientas dedicadas. Las funciones de detección y respuesta a filtraciones son necesarias para cumplir las normativas del Departamento de Servicios Financieros del Estado de Nueva York (DFS), para seguir otras normativas del sector como PCI DSS y, cada vez más, para satisfacer los requisitos clientes de alto perfil que auditan sus bufetes de abogados.

Akamai Guardicore Segmentation: protección completa para aplicaciones críticas

Protección de los datos del cliente: creación de la base para un marco Zero Trust y aplicación de las prácticas recomendadas y la higiene de seguridad de la red en entornos cada vez más complejos e interconectados.

Aislamiento de las aplicaciones críticas de la infraestructura de TI más amplia: segmentación de los activos de gran valor, como un DMS o una aplicación de correo electrónico, con políticas de acordonamiento, lo que reduce la exposición a amenazas tanto dentro como fuera del bufete de abogados.

Adopción de la nube de forma segura y rápida: asignación de cargas de trabajo y elaboración de un inventario de todas las aplicaciones críticas y sus dependencias antes de la migración. Las políticas de acordonamiento utilizan estos mapas como base para una seguridad coherente que siga las cargas de trabajo durante todo el proceso de migración. Este enfoque permite una migración a la nube más rápida y segura de las cargas de trabajo, al tiempo que se mantienen los mismos controles de seguridad.

Garantía de la continuidad del negocio con una mitigación eficaz de las filtraciones: uso de una visibilidad detallada del tráfico de este a oeste y los indicadores de filtración configurados para alertar sobre movimientos anómalos, a fin de detener a los atacantes antes de que el ransomware u otra amenaza paralice la empresa.

Reducción del riesgo mediante la limitación del movimiento lateral: establecimiento de límites internos y acordonamiento de las aplicaciones y los sistemas esenciales para reducir la superficie de ataque. Así se protege eficazmente contra la propagación lateral de los ataques, lo que limita los daños en caso de filtración.

Conclusión

Akamai Guardicore Segmentation proporciona a los bufetes de abogados una solución que les permite visualizar y comprender las conexiones abiertas que podrían utilizarse en un ataque. Además, la solución permite a las empresas proteger esas conexiones mediante la microsegmentación.

Nuestra solución proporciona una cobertura de seguridad completa para las aplicaciones críticas de un bufete de abogados en entornos de TI híbridos, que residen tanto en máquinas virtualizadas como bare metal, y en entornos locales, IaaS o PaaS. Proporciona visibilidad de las dependencias y los flujos de las aplicaciones, permite aplicar políticas de segmentación detalladas y ofrece funciones integradas de detección y respuesta a filtraciones. Estas prestaciones son cruciales para evitar la pérdida de datos y los escenarios de tiempo de inactividad que pueden interrumpir el negocio de un bufete de abogados.

Los bufetes de abogados que utilizan Akamai Guardicore Segmentation pueden comprender mejor su entorno, proteger sus aplicaciones esenciales y reducir drásticamente el impacto y el tiempo de respuesta si un atacante logra introducirse en su red. Además, las funciones de segmentación basadas en software que se proporcionan son mucho más rentables, requieren menos tiempo y son más flexibles y eficaces que las de muchas otras soluciones de segmentación, como los firewalls tradicionales. En rasgos generales, Akamai Guardicore Segmentation es una solución de seguridad líder en el sector que está bien equipada para hacer frente a los desafíos de seguridad de los bufetes de abogados modernos.

Descubra cómo puede proteger los valiosos datos de sus clientes. Obtenga más información sobre nosotros en akamai.com/guardicore.