Akamai

WHITE PAPER

Como proteger a empresa jurídica moderna

Proteção para aplicações críticas e dados do cliente

Introdução

Profissionais da área jurídica lidam com dados confidenciais todos os dias. Com isso em mente, muitas empresas estão investindo em controles de segurança mais avançados e concentrando seus esforços no projeto de seus sistemas e processos de TI em torno do conceito de Zero Trust, para proteger suas aplicações críticas e controlar o acesso do usuário final.

A abordagem Zero Trust implementa um modelo de menor privilégio, garantindo que usuários, sistemas e aplicativos autorizados tenham apenas o acesso apropriado para suas respectivas funções, além de protegendo contra movimentos laterais, ransomware e acesso não autorizado. Uma das maneiras mais flexíveis e seguras de implementar a abordagem Zero Trust é usar a microssegmentação.

Para entender a importância disso, vamos começar analisando um pouco de história.

Violações de alto perfil: um alerta para o setor jurídico

Durante anos, as autoridades federais dos EUA alertaram que as grandes empresas de advocacia são alvos fáceis para os criminosos virtuais porque elas são repositórios de dados corporativos ricos em informações. O FBI começou a alertar empresas de advocacia proeminentes que estavam sendo alvo de criminosos cibernéticos organizados desde 2009. Em 2011, eles convidaram 200 das maiores empresas de advocacia a discutir o aumento de ataques cibernéticos sofisticados direcionados ao setor.

> **Uma das maneiras mais flexíveis e seguras de implementar a abordagem Zero Trust é usar a microssegmentação.**

Desde 2014, mais de 100 empresas de advocacia em 14 Estados relataram violações de dados, de acordo com a Law.com. O Relatório de Pesquisa sobre Tecnologia Legal da American Bar Association de 2022, uma pesquisa anual que explora o uso da tecnologia no setor jurídico, descobriu que mais de um quarto das empresas de advocacia (de todos os portes) sofreram uma violação de segurança. O impacto das violações varia do tempo de inatividade, causado por ransomware, a longas disputas legais após os dados do cliente vazarem na Internet.

Em 2015, o setor jurídico surgiu no ranking anual da Cisco de setores visados pelos hackers pela primeira vez. Como resultado, muitas instituições financeiras começaram a exigir que empresas de advocacia façam auditorias periódicas de suas práticas de segurança cibernética ao realizar negócios juntos.

Em particular, duas violações de peso das empresas de direito internacional Mossack Fonseca & Co e DLA Piper resultaram em um alerta para todo o setor jurídico e financeiro. Em um vazamento apelidado de "Panama Papers", mais de 11 milhões de documentos, mais de quatro décadas de registros, foram vazados da empresa de advocacia offshore Mossack Fonseca & Co. A violação expôs paraísos fiscais e as contas offshore de empresas globais e líderes mundiais influentes, com graves consequências. Em 2018, a empresa anunciou que estava encerrando suas operações, em grande parte devido as consequências da violação. As empresas de advocacia têm uma responsabilidade ética e fiduciária de realizar todos os esforços razoáveis para proteger as informações que possuem. O vazamento de dados "Panama Papers" representa a maior violação até agora de confidencialidade entre uma empresa de advocacia e seus clientes e contribuiu para uma mudança na abordagem de segurança cibernética do setor. No entanto, apesar do foco recém-descoberto em melhorar a postura de segurança, os invasores mostram poucos indícios de estarem desacelerando.

> **Mais de 1 em 4 empresas de advocacia sofreram uma violação de segurança.**
>
> — Relatório da Pesquisa de Tecnologia Legal da American Bar Association 2022

Quase que no mesmo momento do vazamento da Mossack Fonseca & Co, a DLA Piper, uma das empresas de advocacia mais proeminentes do mundo com presença em mais de 40 países, foi vítima de um ataque de malware NotPetya. Isso custou semanas de interrupção, milhões em perda de negócios, custos de recuperação e alguma publicidade muito ruim.

Mais recentemente, após um ataque de ransomware, a Grubman Shire Meiselas & Sacks perdeu 756 gigabytes de dados de sua clientela de alto nível, incluindo Lady Gaga, LeBron James e Madonna. A empresa de advocacia estava relutante em pagar o resgate, o que levou os invasores a vazar informações sobre Lady Gaga e a fazer um leilão do que alegaram serem dados contendo detalhes sobre outros clientes.

Escritórios de advocacia modernos: é hora de adotar soluções modernas de cibersegurança

A maioria das violações descritas envolveu ataques de ameaças persistentes avançadas (APT) que incluíram phishing, malware e ransomware para roubar dados confidenciais de clientes, materiais de fusão, propriedade intelectual e informações financeiras. Atraídos por grandes quantidades de dinheiro, os invasores têm cada vez mais suporte de grupos de crime organizado que fazem investimentos significativos em ferramentas de ataque e equipes profissionais.

> **As empresas que não têm segmentação adequada em seu ambiente de TI correm o risco de ter a cobertura negada em caso de violação de dados.**

Mais clientes agora estão considerando a segurança cibernética como um fator importante para decidir com qual empresa de advocacia negociar atualmente. As empresas que não possuem controles de segurança modernos têm mais probabilidade de perder negócios para empresas que tomaram medidas para melhorar sua postura de segurança e demonstrar seu compromisso com a proteção dos dados dos clientes. Além disso, muitas seguradoras cibernéticas agora estão exigindo alguma forma de segmentação para dados e aplicativos confidenciais. As empresas que não têm segmentação adequada em seu ambiente de TI correm o risco de ter a cobertura negada em caso de violação de dados.

O que está faltando: proteger as aplicações críticas da empresa

Como você pode ver, as empresas de advocacia não são mais o repositório seguro de informações privilegiadas que eram no passado. Atualmente, os criminosos virtuais reconhecem empresas de advocacia como cofres de dados corporativos confidenciais e proprietários que são alvos ideais para ataques de segurança cibernética.

Na verdade, as empresas de advocacia geralmente são percebidas como alvos mais fáceis do que a maioria de seus clientes. É por isso que um invasor que deseja dados específicos de uma empresa geralmente tenta obter esses dados primeiro por meio do seu escritório de advocacia. A natureza sigilosa e a variedade de informações que as empresas de advocacia armazenam, juntamente com seus controles de segurança geralmente mais fracos, fazem delas um alvo lucrativo para os invasores.

Os invasores estão incrivelmente interessados nas informações armazenadas nos aplicativos essenciais aos negócios da empresa de advocacia, principalmente no DMS (Document Management System, sistema de gerenciamento de documentos) e no e-mail. Do ponto de vista da segurança de TI, os aplicativos comerciais mais críticos de uma empresa de advocacia são seus aplicativos de DMS e e-mail. Esses aplicativos detêm a maior parte das informações altamente confidenciais, sensíveis e privilegiadas dos clientes e, em muitos casos, não residem mais apenas em data centers locais.

Os aplicativos DMS oferecem uma ampla variedade de funções e recursos, incluindo uma organização centralizada de arquivos e pastas, gerenciamento de versões, gerenciamento de e-mail, edição de documentos, indexação e pesquisa, gerenciamento de permissões e muito mais. Geralmente, eles são implantados em ambientes de TI heterogêneos com uma combinação de servidores virtualizados e bare-metal e exigem integração com vários outros sistemas com níveis variados de segurança interna. Embora essas integrações possam tornar um DMS mais útil para uma empresa de advocacia, elas também podem torná-lo menos seguro e aumentar drasticamente sua superfície de ataque.

Os pontos de extremidade também se tornaram tão móveis e dinâmicos que as soluções de segurança tradicionais muitas vezes falham na proteção deles, já que, como muitas organizações, as empresas de advocacia concentraram principalmente seus investimentos em ferramentas de segurança no perímetro. Essas soluções não fornecem mais o nível de lei de proteção que as empresas precisam para proteger aplicações críticas. Além disso, a realidade é que muitas empresas de advocacia ainda não têm os controles necessários para detectar ou impedir que um invasor se mova lateralmente e acesse sistemas de dados confidenciais quando um agente de ameaça acessar a rede por meio de um ponto de extremidade comprometido.

Devido a todos esses desafios, muitas empresas de advocacia modernas estão começando a investir em uma nova geração de soluções de cibersegurança capazes de atender às suas necessidades únicas e em constante mudança. A segmentação baseada em software, especificamente a microssegmentação, oferece suporte a uma abordagem Zero Trust para proteger aplicativos e dados críticos, fornecendo uma abordagem mais granular ao controle de comunicações dentro da rede, permitindo que apenas os usuários e sistemas autorizados se comuniquem com aplicações críticas. Isso torna muito mais difícil para um invasor mover-se lateralmente pela rede, limitando o escopo de uma possível violação.

A COVID-19 tornou as coisas ainda mais desafiadoras:

- Muitas empresas de advocacia migraram para o trabalho remoto
- Por isso, os funcionários não estão mais conectados à rede a partir de seu escritório corporativo, mas sim de redes domésticas desprotegidas
- O aumento do uso de soluções de VPN e VDI tornou a implementação de políticas de segurança e a atribuição de tráfego de rede a usuários autorizados ainda mais desafiadora

Quatro maneiras pelas quais a Akamai ajuda as empresas de advocacia a proteger os dados dos clientes

Visibilidade completa

Obtenha visibilidade abrangente da carga de trabalho para entender todas as conexões abertas com aplicativos que armazenam dados confidenciais.

Controle de acesso do usuário

Implemente políticas que controlem o acesso a aplicativos e dados, independentemente de onde eles estejam: No local ou na nuvem.

Segmentação baseada em software

Faça a microssegmentação rápida e flexível de aplicações críticas, como DMS e e-mail, para limitar a exposição em caso de violação.

Detecção e prevenção a ameaças

Combine segmentação dinâmica e recursos de fraude para detectar e conter violações ativas e proteger os dados do cliente.

Proteção unificada com a Akamai Guardicore Segmentation

A Akamai Guardicore Segmentation oferece a solução de microssegmentação mais abrangente do setor para proteger aplicações críticas para os negócios. Ela acelera drasticamente a implementação de políticas de segmentação, simplifica a manutenção contínua e, em última análise, é mais eficaz na atenuação de ameaças que dependem do movimento lateral para obter sucesso.

> **Para proteger melhor os dados do cliente, muitas empresas de advocacia estão buscando soluções como a microssegmentação para implementar uma abordagem mais granular ao controle de comunicações dentro da rede, permitindo que apenas os usuários e sistemas autorizados se comuniquem com aplicações críticas.**

Nossa solução fornece um mapa visual de todos os aplicativos e outros ativos em seu data center, juntamente com suas dependências. Os operadores de segurança podem então criar e aplicar políticas de segurança em nível de rede e de processo de forma rápida e intuitiva para isolar e segmentar seus aplicativos e ativos críticos. Essa abordagem definida por software para segmentação é independente da infraestrutura subjacente, permitindo que ela proteja consistentemente cargas de trabalho que abrangem sistemas locais (legados e modernos), VMs, contêineres, nuvens e dispositivos.

As políticas podem ser criadas em torno de aplicativos individuais ou logicamente agrupados, independentemente de onde residem no data center. Essas políticas determinam quais aplicativos podem e não podem se comunicar entre si, oferecendo suporte a uma abordagem Zero Trust. Outro recurso importante exclusivo da Akamai Guardicore Segmentation é nossa detecção e resposta de violação integrada, o que reduz a complexidade do gerenciamento de várias ferramentas dedicadas. A detecção e a resposta a violações são necessárias para cumprir as normas do Departamento de Serviços financeiros (DFS) do Estado de Nova York, outros mandatos do setor, como o PCI DSS, e cada vez mais por clientes de alto nível que auditam suas empresas de advocacia.

Akamai Guardicore Segmentation: proteção abrangente para aplicações críticas

Proteja os dados de clientes: crie a base para uma estrutura Zero Trust e imponha a higiene da segurança de rede e as práticas recomendadas, em ambientes cada vez mais complexos e interconectados.

Isole as aplicações críticas da infraestrutura de TI mais ampla: segmente ativos de alto valor, como um DMS ou aplicativo de e-mail, com políticas de proteção virtual, reduzindo a exposição a ameaças de dentro e de fora de um escritório de advocacia.

Adote a nuvem com segurança e rapidez: mapeie cargas de trabalho e faça o inventário de todas as aplicações críticas e suas dependências antes da migração. As políticas de delimitação usam esses mapas como base para uma segurança consistente que segue as cargas de trabalho durante todo o processo de migração. Essa abordagem permite a migração mais rápida e segura de cargas de trabalho para a nuvem, mantendo os mesmos controles de segurança em vigor.

Garanta a continuidade dos negócios com atenuação eficiente de violações: use visibilidade granular do tráfego leste-oeste, e indicadores de violação definidos para alertar sobre movimentos anormais, para impedir os agentes de ameaça antes que o ransomware ou outra ameaça interrompa os negócios.

Reduza os riscos limitando o movimento lateral: defina limites internos e delimite o acesso a aplicações e sistemas críticos para os negócios para reduzir a superfície de ataque. Isso protege efetivamente contra a disseminação lateral de ataques, limitando os danos em caso de violação.

Conclusão

A Akamai Guardicore Segmentation oferece às empresas de advocacia uma solução que permite visualizar e entender as conexões abertas que podem ser usadas em um ataque. Além disso, a solução permite que as empresas protejam essas conexões usando microssegmentação.

Nossa solução oferece cobertura de segurança abrangente para as aplicações críticas de uma empresa de advocacia em ambientes de TI híbridos, residentes em máquinas virtualizadas e bare-metal e em IaaS ou PaaS locais. Ela oferece visibilidade das dependências e dos fluxos de aplicativos, aplicação de políticas de segmentação granular e detecção e resposta de violação integradas. Esses recursos são cruciais para evitar a perda de dados e cenários de tempo de inatividade dos negócios que podem prejudicar os negócios de um escritório de advocacia.

As empresas de advocacia que usam a Akamai Guardicore Segmentation podem entender melhor seu ambiente, proteger suas aplicações críticas e reduzir drasticamente o impacto e o tempo de resposta em caso de violação. Além disso, os recursos de segmentação baseados em software fornecidos são significativamente mais econômicos, menos demorados, mais flexíveis e mais eficientes do que aqueles de muitas outras soluções de segmentação, como firewalls tradicionais. Em geral, a Akamai Guardicore Segmentation é uma solução de segurança líder do setor, bem equipada para atender aos desafios de segurança da empresa moderna de advocacia.

Descubra como você pode proteger os dados valiosos de seus clientes. Saiba mais sobre nós em akamai.com/guardicore.