Akamai

LIVRE BLANC

Sécuriser les cabinets juridiques d'aujourd'hui

Protection des applications critiques et des données client

Introduction

Les professionnels du droit traitent des données sensibles chaque jour dans le cadre de leurs activités. Dans ce contexte, de nombreux cabinets investissent dans des contrôles de sécurité plus avancés en privilégiant le concept de Zero Trust lors de la conception de leurs systèmes et processus informatiques pour sécuriser leurs applications critiques et contrôler les accès de leurs utilisateurs finaux.

La stratégie Zero Trust met en œuvre un modèle de moindre privilège en vertu duquel seuls les utilisateurs, systèmes et applications autorisés ont l'accès correspondant à leurs fonctions respectives, en assurant également une protection contre les mouvements latéraux, les attaques par ransomware et les accès non autorisés. L'une des façons les plus flexibles et les plus sûres de mettre en œuvre l'approche Zero Trust consiste à utiliser la microsegmentation.

Pour bien comprendre toute l'importance de cette technique de sécurité, nous allons commencer par un peu d'histoire.

Violations de grande envergure : un signal d'alarme pour le secteur juridique

Depuis des années, les autorités fédérales américaines alertent sur le fait que les grands cabinets juridiques sont des cibles faciles pour les cybercriminels en raison des grandes quantités d'informations stockées dans les référentiels de données d'entreprise qu'ils détiennent. Le FBI commençait déjà dès le début de l'année 2009 à avertir d'importants cabinets juridiques qu'ils étaient ciblés par des cybercriminels organisés. En 2011, il a même invité 200 des plus grands cabinets juridiques à discuter de la montée des cyberattaques sophistiquées ciblant le secteur.

> **L'une des façons les plus flexibles et les plus sûres de mettre en œuvre l'approche Zero Trust consiste à utiliser la microsegmentation.**

Selon Law.com, plus de 100 cabinets juridiques dans 14 États américains ont signalé des violations de données depuis 2014. L'enquête annuelle de l'American Bar Association sur l'utilisation des technologies dans le secteur juridique, publiée dans son rapport de 2022 (sous le titre original 2022 Legal Technology Survey Report), a révélé que plus d'un quart des cabinets juridiques (toutes tailles confondues) ont subi une violation de sécurité. Ces attaques provoquent des perturbations de différentes natures, allant des interruptions de service causées par des ransomwares à des contentieux juridiques complexes après la divulgation de données de clients en ligne.

En 2015, le secteur juridique est apparu pour la première fois dans le classement annuel des industries ciblées par les pirates informatiques de Cisco. En conséquence, de nombreuses institutions financières ont commencé à exiger des cabinets juridiques qu'ils soumettent leurs pratiques de cybersécurité à des audits réguliers dès lors qu'ils traitent ensemble.

Ce sont notamment les deux violations massives dont ont été victimes les cabinets juridiques internationaux Mossack Fonseca & Co et DLA Piper qui auront eu l'effet d'un électrochoc pour l'ensemble de l'industrie juridique et financière. Dans l'affaire dite des « Panama Papers », plus de 11 millions de documents, représentant plus de quatre décennies de dossiers, ont fuité du cabinet juridique offshore Mossack Fonseca & Co. Cette violation, qui a eu de graves conséquences, a révélé publiquement que des sociétés internationales et des dirigeants influents du monde entier possédaient des comptes offshore dans des paradis fiscaux. Le cabinet a annoncé sa fermeture en 2018, essentiellement en raison des répercussions de cette faille de sécurité. Les cabinets juridiques sont tenus, pour des raisons éthiques et fiduciaires, de déployer toutes les mesures raisonnables nécessaires pour protéger les informations qu'ils détiennent. La fuite de données de l'affaire des « Panama Papers » représente à ce jour la violation la plus importante du principe du secret professionnel liant un cabinet juridique à ses clients et a contribué à modifier l'approche du secteur en matière de cybersécurité. Néanmoins, en dépit des efforts nouvellement déployés pour améliorer les mécanismes de sécurité, les activités des cybercriminels ne montrent que très peu de signes de ralentissement.

> **Plus d'un cabinet juridique sur quatre a été victime d'une violation de sécurité.**
>
> — American Bar Association Legal Technology Survey Report 2022

Presque simultanément à la fuite de données de Mossack Fonseca & Co, DLA Piper, l'un des cabinets juridiques les plus importants au monde avec une présence dans plus de 40 pays, a été victime d'une attaque par le logiciel malveillant NotPetya. Cette faille de sécurité a perturbé le fonctionnement du cabinet pendant des semaines, lui a coûté des millions de dollars en pertes d'activité et en coûts de rétablissement, sans omettre la très mauvaise publicité dont il a fait l'objet.

Plus récemment, à la suite d'une attaque par ransomware, le cabinet Grubman Shire Meiselas & Sacks a perdu 756 gigaoctets de données relatives à certains de ses clients les plus prestigieux, dont Lady Gaga, LeBron James et Madonna. La réticence du cabinet juridique à payer la rançon a conduit les hackers à divulguer des informations sur Lady Gaga et à mettre aux enchères ce qu'ils prétendaient être des données contenant des renseignements sur d'autres clients.

Il est temps pour les cabinets juridiques modernes d'adopter des solutions de cybersécurité modernes

La majorité des violations décrites ont consisté en des attaques par menaces persistantes avancées (APT) de type hameçonnage, logiciel malveillant et ransomware dont le but était de voler des données sensibles sur les clients, des documents portant sur des fusions, des éléments de propriété intellectuelle et des informations financières. En raison des sommes considérables en jeu, les pirates sont de plus en plus souvent soutenus par des groupes criminels organisés qui investissent massivement dans des équipements d'attaque et dans des équipes de spécialistes.

> **Les cabinets dont l'environnement informatique n'est pas segmenté de manière adéquate encourent le risque de voir leur demande d'indemnisation rejetée en cas de violation de données.**

De plus en plus de clients considèrent désormais la question de la cybersécurité comme un critère déterminant dans leur choix d'un cabinet juridique. Les cabinets qui n'offrent pas de contrôles de sécurité modernes courent davantage le risque de se faire ravir leur clientèle par ceux qui ont su prendre des mesures pour renforcer leur position en matière de sécurité et démontrer leur engagement à sécuriser les données de leurs clients. Par ailleurs, de nombreuses compagnies d'assurance couvrant les cyber-risques exigent désormais la mise en œuvre d'une certaine forme de segmentation pour les données et les applications sensibles. Les cabinets dont l'environnement informatique n'est pas segmenté de manière adéquate s'exposent au risque de voir leur demande d'indemnisation rejetée en cas de violation de données.

La sécurisation des applications critiques, une priorité pour les cabinets

On constate donc aujourd'hui qu'il peut arriver à des cabinets juridiques de manquer quelque peu à leur réputation de dépositaires d'informations protégées. Aujourd'hui, les cybercriminels voient les cabinets juridiques comme des coffres-forts où sont conservées des données d'entreprise confidentielles et sensibles, qui constituent des cibles de choix pour les attaques de cybersécurité.

D'ailleurs, les cabinets juridiques sont souvent perçus comme des cibles plus faciles que la plupart de leurs propres clients. C'est pourquoi un hacker qui souhaite obtenir des données spécifiques au sujet d'une entreprise essaiera souvent d'obtenir ces données par l'intermédiaire de son cabinet juridique en premier lieu. La nature sensible et la diversité des informations que détiennent les cabinets juridiques, ce à quoi s'ajoutent des contrôles de sécurité en général moins rigoureux, en font une cible lucrative pour les cybercriminels.

Les pirates s'intéressent tout particulièrement aux informations stockées dans les applications stratégiques des cabinets juridiques, notamment dans leurs systèmes de gestion des documents et de messagerie électronique. Du point de vue de la sécurité informatique, les systèmes de gestion des documents et de messagerie électronique constituent les applications les plus stratégiques des cabinets juridiques. Ces applications renferment la majeure partie des informations hautement confidentielles, sensibles et privilégiées des clients, dans bien des cas, elles ne sont plus uniquement hébergées dans des centres de données sur site.

Les applications de gestion des documents offrent un large éventail de fonctions et de caractéristiques, dont l'organisation centralisée des fichiers et dossiers, la gestion des versions, la gestion des e-mails, la modification de documents, l'indexation et la recherche, gestion des autorisations, et bien plus encore. Elles sont souvent déployées dans des environnements informatiques hétérogènes avec une combinaison de serveurs virtualisés et bare metal, et nécessitent une intégration à plusieurs autres systèmes avec différents niveaux de sécurité interne. Si ces intégrations sont susceptibles d'accroître l'utilité du système de gestion des documents d'un cabinet juridique, elles peuvent également le rendre moins sûr et augmenter considérablement sa surface d'attaque.

De plus, les points de terminaison sont également devenus si mobiles et dynamiques aujourd'hui que les solutions de sécurité traditionnelles ne parviennent plus à protéger les cabinets juridiques que dans de rares cas, dans la mesure où ces derniers, à l'instar de nombreuses entreprises, ont principalement concentré leurs investissements dans des outils destinés à assurer une sécurité basée sur leur périmètre réseau. Ces solutions n'offrent plus le niveau de protection dont les cabinets juridiques ont besoin pour sécuriser leurs applications critiques. En outre, il s'avère que de nombreux cabinets juridiques ne disposent toujours pas des contrôles nécessaires pour détecter un hacker ou l'empêcher d'attaquer par mouvement latéral et d'accéder à des systèmes de données sensibles dès lors qu'un acteur malveillant accède au réseau par le biais d'un point de terminaison compromis.

Compte tenu de tous ces défis, de nombreux cabinets juridiques commencent désormais à investir dans une nouvelle génération de solutions de cybersécurité en mesure de répondre à leurs besoins uniques et évolutifs. La segmentation logicielle, notamment la microsegmentation, intègre une stratégie Zero Trust pour sécuriser les applications et les données critiques en fournissant une approche plus granulaire du contrôle des communications au sein du réseau, qui permet uniquement à des utilisateurs et systèmes autorisés de communiquer avec les applications critiques. Il devient donc beaucoup plus difficile pour un hacker d'attaquer par mouvement latéral votre réseau, ce qui limite la portée d'une violation potentielle.

La pandémie du COVID-19 est venue compliquer encore davantage la situation :

- De nombreux cabinets juridiques sont passés au travail à distance.
- De ce fait, les collaborateurs ne se connectent plus au réseau depuis leur cabinet, mais depuis des réseaux domestiques non sécurisés.
- En raison de la multiplication des solutions VPN et VDI, il est devenu encore plus difficile de mettre en œuvre des politiques de sécurité et de répartir le trafic réseau entre les utilisateurs autorisés.

Akamai protège les données des clients des cabinets juridiques grâce à quatre techniques

Une visibilité totale

Bénéficiez d'une visibilité complète des charges de travail pour comprendre toutes les connexions ouvertes à des applications hébergeant des données sensibles.

Un contrôle des accès utilisateur

Mettez en œuvre des règles qui contrôlent l'accès aux applications et aux données, quel que soit l'endroit où elles se trouvent, sur site ou dans le cloud.

Une segmentation logicielle

Microsegmentez rapidement et de manière flexible les applications critiques comme les systèmes de gestion de documents et de messagerie afin de limiter votre exposition en cas de violation.

Une détection et prévention des menaces

Combinez la segmentation dynamique et les fonctionnalités de leurre pour détecter et contenir les violations actives et protéger les données de vos clients.

Une protection unifiée avec Akamai Guardicore Segmentation

Akamai Guardicore Segmentation se présente comme la solution de microsegmentation la plus complète du marché pour protéger les applications stratégiques. Elle accélère de manière considérable la mise en œuvre des règles de segmentation, simplifie la maintenance continue et est en définitive plus efficace pour atténuer les menaces qui reposent sur des mouvements latéraux.

> **Pour mieux protéger les données des clients, de nombreux cabinets juridiques se tournent vers des solutions comme la microsegmentation pour mettre en œuvre une approche plus granulaire du contrôle des communications au sein de leur réseau, qui permet uniquement à des utilisateurs et systèmes autorisés de communiquer avec les applications critiques.**

Notre solution fournit une carte visuelle de toutes les applications et d'autres actifs de votre centre de données, ainsi que de leurs dépendances. Les opérateurs de sécurité peuvent ensuite créer et appliquer de façon rapide et intuitive des règles de sécurité au niveau du réseau et des processus pour isoler et segmenter leurs applications et ressources critiques. Cette approche de segmentation logicielle est indépendante de l'infrastructure sous-jacente, ce qui lui permet de protéger de manière cohérente les charges de travail aussi bien des systèmes sur site (hérités et récents) que sur des machines virtuelles, des conteneurs, des plateformes cloud et des terminaux.

Des règles peuvent être créées autour d'applications individuelles ou groupées logiquement, quel que soit l'endroit où elles sont hébergées dans le centre de données. Ces règles déterminent les applications qui peuvent et ne peuvent pas communiquer entre elles en adoptant une approche Zero Trust. La fonctionnalité intégrée de détection des violations et de réponse aux incidents, qui évite d'avoir à gérer plusieurs outils dédiés, est une autre fonctionnalité importante exclusive d'Akamai Guardicore Segmentation. Des mesures de détection des violations et de réponse aux incidents sont nécessaires pour se conformer aux réglementations du Département des services financiers de l'État de New York (DFS), à d'autres prescriptions industrielles comme la norme PCI DSS et, de plus en plus, aux audits des cabinets juridiques menés par des clients prestigieux.

Akamai Guardicore Segmentation : protection complète pour les applications critiques

Protégez les données client : créez les bases d'un cadre Zero Trust et appliquez l'hygiène et les meilleures pratiques de sécurité réseau dans des environnements de plus en plus complexes et interconnectés.

Isolez les applications critiques de l'infrastructure informatique au sens large : segmentez les actifs à forte valeur ajoutée, comme le système de gestion des documents ou l'application de messagerie électronique, avec des règles de cloisonnement, ce qui permet de réduire l'exposition du cabinet juridique à des menaces internes et externes.

Adoptez le cloud rapidement et en toute sécurité : mappez les charges de travail et faites l'inventaire de toutes les applications critiques et de leurs dépendances avant la migration. Les règles de cloisonnement utilisent ces cartes comme base d'une sécurité cohérente qui suit les charges de travail tout au long du processus de migration. Cette approche permet de mettre en place une migration plus rapide et plus sécurisée des charges de travail dans le cloud, tout en conservant les mêmes contrôles de sécurité.

Assurez la continuité de l'activité grâce à une atténuation efficace des violations : utilisez une visibilité granulaire du trafic est-ouest et des indicateurs de violation configurés pour vous alerter en cas de mouvement anormal, et pour arrêter les acteurs malveillants avant que le ransomware ou une autre menace ne paralyse vos activités.

Limitez les mouvements latéraux pour réduire les risques : définissez des limites internes et cloisonnez les systèmes et applications stratégiques pour réduire la surface d'attaque. Cette approche protège efficacement contre la propagation latérale des attaques et permet de limiter les dégâts en cas de violation.

Conclusion

Akamai Guardicore Segmentation fournit aux cabinets juridiques une solution qui leur donne les moyens de visualiser et de comprendre les connexions ouvertes susceptibles d'être utilisées lors d'une attaque. De plus, la solution permet aux cabinets de sécuriser ces connexions en utilisant la microsegmentation.

Notre solution fournit une couverture de sécurité complète pour les applications critiques des cabinets juridiques dans des environnements informatiques hybrides, hébergées sur des machines virtualisées et bare metal, sur site, ou dans le cadre de services informatiques selon le modèle IaaS ou PaaS. Elle offre une visibilité sur les dépendances et les flux des applications, des règles de segmentation granulaires et une fonctionnalité intégrée de détection des violations et de réponse aux incidents. Ces caractéristiques sont essentielles pour prévenir les scénarios de perte de données et de temps d'arrêt susceptibles de perturber les activités des cabinets juridiques.

Les cabinets juridiques qui utilisent Akamai Guardicore Segmentation sont davantage en mesure de comprendre leur environnement, de sécuriser leurs applications critiques et de réduire considérablement l'impact et le temps de réponse en cas de violation. En outre, notre solution propose des capacités de segmentation logicielle beaucoup plus avantageuses sur le plan économique, moins exigeantes en termes de temps, plus flexibles et plus efficaces que de nombreuses autres solutions de segmentation, notamment les pare-feux traditionnels. Dans l'ensemble, Akamai Guardicore Segmentation constitue une solution de sécurité de pointe dans le secteur, parfaitement conçue pour répondre aux défis de sécurité des cabinets juridiques d'aujourd'hui.

Découvrez comment protéger les données précieuses de vos clients. Pour en savoir plus, consultez notre site à l'adresse akamai.com/guardicore.