Akamai

WHITE PAPER

La sicurezza dei moderni studi legali

Protezione dei dati dei clienti e delle applicazioni di importanza critica

Introduzione

I professionisti del settore legale gestiscono ogni giorno dati sensibili. Per questo motivo, molti studi legali stanno investendo in controlli di sicurezza più avanzati, concentrandosi sulla progettazione di sistemi e processi IT basati sul concetto Zero Trust per proteggere le loro applicazioni di importanza critica e controllare gli accessi degli utenti finali.

L'approccio Zero Trust si basa sul principio del privilegio minimo, garantendo che solo le applicazioni, i sistemi e gli utenti autorizzati possano accedere alle rispettive funzioni, proteggendo, al contempo, da movimenti laterali, attacchi ransomware e accessi non autorizzati. Uno dei modi più flessibili e sicuri per implementare l'approccio Zero Trust è l'utilizzo della microsegmentazione.

Per capire perché questa tecnologia è importante, iniziamo ad esaminare alcuni aspetti importanti.

Violazioni di alto profilo: un campanello di allarme per il settore legale

Da anni, le autorità federali statunitensi avvisano sul fatto che i grandi studi legali sono un facile bersaglio per i criminali informatici, perché ospitano archivi di dati aziendali ricchi di informazioni. L'FBI ha iniziato ad avvisare i più importanti studi legali presi di mira da criminali informatici organizzati già nel 2009, fino ad invitare, nel 2011, 200 tra i principali studi legali a discutere sull'aumento di attacchi informatici sempre più complessi che colpiscono il loro settore.

> **Uno dei modi più flessibili e sicuri per implementare l'approccio Zero Trust è l'utilizzo della microsegmentazione.**

Secondo Law.com, dal 2014 più di 100 studi legali in 14 stati hanno segnalato violazioni di dati. Il Legal Technology Survey Report 2022 dell'American Bar Association, un'indagine annuale che analizza l'uso della tecnologia nel settore legale, ha rivelato che più di un quarto degli studi legali (di tutte le dimensioni) ha subito una violazione della sicurezza. L'impatto delle violazioni spazia da problemi di downtime, causati dal ransomware, alle lunghe controversie legali che seguono alla pubblicazione dei dati dei clienti su Internet.

Nel 2015, il settore legale è apparso per la prima volta nella classifica annuale di Cisco tra i settori presi di mira dagli hacker. Di conseguenza, molti istituti finanziari hanno iniziato a richiedere agli studi legali di sottoporsi a verifiche periodiche sulle loro pratiche di cybersicurezza prima di collaborare con loro.

In particolare, due imponenti violazioni degli studi legali internazionali Mossack Fonseca & Co e DLA Piper hanno fatto scattare un campanello di allarme nell'intero settore finanziario-legale. In una fuga di notizie denominata "Panama Papers", sono trafugati più di 11 milioni di documenti, contenenti oltre quattro decenni di dati, dallo studio legale offshore Mossack Fonseca & Co. La violazione ha messo in luce i paradisi fiscali e i conti offshore di aziende globali e di influenti leader mondiali, con gravi conseguenze finanziarie. Nel 2018, lo studio ha annunciato la sua chiusura, soprattutto a causa delle conseguenze derivate da questa violazione. Gli studi legali hanno la responsabilità etica e fiduciaria di compiere ogni ragionevole sforzo nell'intento di proteggere le informazioni in loro possesso. La fuga di dati "Panama Papers" rappresenta finora la più grande violazione di informazioni riservate dei clienti di uno studio legale e ha contribuito a cambiare l'approccio di questo settore nei confronti della cybersicurezza. Tuttavia, nonostante una nuova attenzione al miglioramento della strategia di sicurezza da parte delle aziende, i criminali non mostrano segni di rallentamento.

> **Più di 1 studio legale su 4 ha subito una violazione della sicurezza.**
>
> — Legal Technology Survey Report 2022 dell'American Bar Association

Quasi contemporaneamente alla fuga di dati di Mossack Fonseca & Co, DLA Piper, uno degli studi legali più importanti al mondo, con una presenza in oltre 40 Paesi, ha subito un attacco malware NotPetya, che è costato all'azienda un'interruzione delle sue attività per settimane con milioni di perdite in termini finanziari e costi per il recupero dei dati, oltre che ad una pessima pubblicità.

Più di recente, in seguito a un attacco ransomware, Grubman Shire Meiselas & Sacks ha perso 756 gigabyte di dati dei suoi clienti più importanti, tra cui Lady Gaga, LeBron James e Madonna. Lo studio legale, mostrandosi riluttante a pagare il riscatto richiesto, ha indotto i criminali a far trapelare informazioni su Lady Gaga e a mettere all'asta dati contenenti dettagli su altri clienti.

Per i moderni studi legali, è tempo di adottare moderne soluzioni per la cybersicurezza

La maggior parte delle violazioni evidenziate ha riguardato attacchi di tipo APT (Advanced Persistent Threat), tra cui phishing, malware e ransomware, sferrati con l'intento di rubare dati sensibili dei clienti, materiali su fusioni, proprietà intellettuale e informazioni finanziarie. Attirati da enormi somme di denaro, i criminali sono sempre più supportati da gruppi criminali organizzati, che investono in modo significativo in strumenti di attacco e team di professionisti.

> **Le aziende che non dispongono di un'adeguata segmentazione del proprio ambiente IT rischiano di vedersi negare la copertura in caso di violazione dei dati.**

Un numero sempre maggiore di clienti inizia ora a considerare la cybersicurezza come un fattore importante nella scelta del proprio studio legale. Le aziende che non dispongono di moderni controlli di sicurezza hanno maggiori probabilità di perdere affari rispetto alle imprese che hanno già adottato misure tali da migliorare la loro strategia di sicurezza e dimostrare il loro impegno nella protezione dei dati dei propri clienti. Inoltre, molte compagnie assicurative che operano nel settore informatico ora richiedono una forma di segmentazione per i dati e le applicazioni sensibili. Le aziende che non dispongono di un'adeguata segmentazione del proprio ambiente IT rischiano di vedersi negare la copertura in caso di violazione dei dati.

Cosa manca: la protezione delle applicazioni di importanza critica negli studi legali

Come si può notare, gli studi legali non possono più garantire l'archivio sicuro di informazioni riservate come una volta. Oggi, i criminali informatici prendono di mira gli studi legali perché dispongono di dati aziendali proprietari e sensibili, rendendoli obiettivi ideali per gli attacchi alla cybersicurezza.

In effetti, gli studi legali sono spesso percepiti come obiettivi più facili da colpire rispetto alla maggior parte dei loro clienti. Ecco perché un criminale cerca prima di ottenere i dati di un'azienda tramite il suo studio legale. La natura sensibile e la varietà di informazioni conservate dagli studi legali, associate ai controlli di sicurezza generalmente più deboli, li rendono un obiettivo redditizio per i criminali,

che sono fortemente interessati alle informazioni memorizzate nelle applicazioni business-critical degli studi legali, in particolare il sistema di gestione dei documenti (DMS) e la posta elettronica. Dal punto di vista della sicurezza informatica, le applicazioni aziendali più critiche per uno studio legale sono i sistemi DMS e la posta elettronica perché contengono la maggior parte delle informazioni altamente riservate, sensibili e confidenziali dei clienti e, in molti casi, non risiedono più solo nei data center on-premise.

Le applicazioni DMS offrono un'ampia gamma di caratteristiche e funzionalità, tra cui l'organizzazione centralizzata di file e cartelle, la gestione di versioni, e-mail e autorizzazioni, la modifica dei documenti, l'indicizzazione e la ricerca e molto altro. Spesso, queste applicazioni vengono distribuite in ambienti IT eterogenei, con un mix di server virtualizzati e bare metal, e richiedono l'integrazione con altri sistemi che presentano vari livelli di sicurezza interna. Se è vero che queste integrazioni possono rendere un sistema DMS più utile per uno studio legale, d'altro canto possono diminuirne la sicurezza e aumentare drasticamente la sua superficie di attacco.

Gli endpoint sono diventati così mobili e dinamici che le soluzioni di sicurezza tradizionali spesso non riescono a proteggerli, poiché, come molte organizzazioni, gli studi legali hanno concentrato i loro investimenti in strumenti di sicurezza principalmente sul perimetro. Queste soluzioni non forniscono più il livello di protezione di cui gli studi legali hanno bisogno per proteggere le loro applicazioni critiche. Inoltre, la verità è che molti studi legali non dispongono ancora dei controlli necessari per rilevare o impedire a un criminale di spostarsi lateralmente e di accedere ai sistemi di dati sensibili una volta ottenuto l'accesso alla rete tramite un endpoint compromesso.

Considerate tutte queste sfide, molti studi legali moderni stanno iniziando a investire in una nuova generazione di soluzioni per la cybersicurezza in grado di rispondere alle loro esclusive esigenze in continua evoluzione. La segmentazione basata su software, in particolare la microsegmentazione, supporta un approccio Zero Trust alla protezione delle applicazioni e dei dati critici, fornendo un approccio più granulare al controllo delle comunicazioni all'interno della rete per consentire solo agli utenti e ai sistemi autorizzati di comunicare con le applicazioni critiche. In tal modo, diventa molto più difficile per un criminale spostarsi lateralmente all'interno della rete, il che limita la portata di una potenziale violazione.

Il COVID-19 ha reso le cose ancora più difficili:

- Molti studi legali sono passati al telelavoro.
- Per questo motivo, i dipendenti non si collegano più alla rete dall'ufficio aziendale, ma da reti domestiche non sicure
- L'aumento dell'uso di soluzioni VPN e VDI ha reso ancora più difficile l'implementazione di policy di sicurezza e l'attribuzione del traffico di rete agli utenti autorizzati

Quattro modi con cui Akamai aiuta gli studi legali a proteggere i dati dei loro clienti

Visibilità completa

Ottenete una visibilità completa dei carichi di lavoro per comprendere tutte le connessioni aperte alle applicazioni che ospitano dati sensibili.

Controllo degli accessi degli utenti

Implementate le policy appropriate per controllare l'accesso alle applicazioni e ai dati necessari, indipendentemente dalla loro posizione, on-premise o nel cloud.

Segmentazione basata sul software

Microsegmentazione rapida e flessibile di applicazioni critiche, come sistemi DMS e posta elettronica, per limitare l'esposizione in caso di violazioni.

Rilevamento e prevenzione delle minacce

Combinate la segmentazione dinamica e le funzionalità di individuazione necessarie per rilevare e contenere le violazioni attive e per proteggere i dati dei clienti.

Protezione unificata con Akamai Guardicore Segmentation

Akamai Guardicore Segmentation offre la soluzione di microsegmentazione più completa del settore per la protezione delle applicazioni business-critical. Accelera drasticamente l'implementazione delle policy di segmentazione, semplifica la manutenzione continua e risulta, in definitiva, più efficace nella mitigazione delle minacce che si basano sul movimento laterale.

> **Per proteggere meglio i dati dei loro clienti, molti studi legali si rivolgono a soluzioni specifiche come la microsegmentazione per implementare un approccio più granulare al controllo delle comunicazioni all'interno della rete in modo da consentire solo agli utenti e ai sistemi autorizzati di comunicare con le applicazioni di importanza critica.**

La nostra soluzione fornisce una mappa visiva di tutte le applicazioni e delle altre risorse presenti nel vostro data center, insieme alle loro dipendenze. Gli addetti alla sicurezza possono, quindi, creare e applicare in modo rapido e intuitivo policy di sicurezza a livello di rete e di processo per isolare e segmentare le applicazioni e le risorse critiche. Questo approccio alla segmentazione definito da software è indipendente dall'infrastruttura sottostante al fine di proteggere in modo coerente i carichi di lavoro distribuiti tra i sistemi on-premise (sia legacy che moderni), le VM, i container, i cloud e i dispositivi.

Potete creare policy relative a singole applicazioni o ad applicazioni raggruppate logicamente, indipendentemente dalle posizioni in cui risiedono nel data center. Queste policy indicano quali applicazioni possono o meno comunicare tra loro a supporto di un effettivo approccio Zero Trust. Un'altra importante funzionalità esclusiva di Akamai Guardicore Segmentation è rappresentata dalle funzioni integrate di rilevamento e risposta alle violazioni, che riducono la complessità della gestione di più strumenti dedicati. Le operazioni di rilevamento e risposta alle violazioni sono richieste per conformarsi alle normative del Dipartimento dei servizi finanziari (DFS) dello Stato di New York, ai requisiti normativi di altri settori come il PCI DSS e, sempre più spesso, ai clienti di alto profilo che controllano i loro studi legali.

Akamai Guardicore Segmentation: una protezione completa per le applicazioni di importanza critica

Proteggere i dati dei clienti: create le basi per un sistema Zero Trust e applicate le procedure e le best practice per la sicurezza di rete in ambienti sempre più complessi e interconnessi.

Isolare le applicazioni di importanza critica dall'infrastruttura IT più ampia: segmentate le risorse di alto valore, come un sistema DMS o un'applicazione di posta elettronica, con policy di isolamento delle applicazioni, riducendo l'esposizione alle minacce provenienti sia dall'interno che dall'esterno dello studio legale.

Adottare il cloud in modo sicuro e rapido: mappate i carichi di lavoro e inventariate tutte le applicazioni di importanza critica insieme alle loro dipendenze prima di effettuare la migrazione. Le policy di isolamento delle applicazioni utilizzano queste mappe come fondamenta per garantire una sicurezza coerente dei carichi di lavoro per tutto il processo di migrazione. Questo approccio offre una migrazione più rapida e sicura dei carichi di lavoro nel cloud, mantenendo gli stessi controlli di sicurezza.

Assicurare la continuità aziendale con un'efficiente mitigazione delle violazioni: utilizzate la visibilità granulare del traffico est-ovest e gli indicatori di violazione impostati per avvisare in caso di movimenti anomali in modo da bloccare i criminali prima che il ransomware o un'altra minaccia riescano a interrompere le attività aziendali.

Ridurre il rischio limitando il movimento laterale: stabilite confini interni e isolate le applicazioni e i sistemi business-critical per ridurre la superficie di attacco in modo da proteggere efficacemente dalla diffusione laterale degli attacchi, limitando i danni in caso di violazione.

Conclusione

Akamai Guardicore Segmentation offre agli studi legali una soluzione che consente di visualizzare e comprendere le connessioni aperte potenzialmente utilizzabili in un attacco e di proteggerle tramite la microsegmentazione.

La nostra soluzione fornisce una sicurezza completa per le applicazioni critiche di uno studio legale in ambienti IT ibridi, che risiedono sia su computer virtualizzati che bare metal e su applicazioni on-premise, IaaS o PaaS. La soluzione offre visibilità sulle dipendenze e sui flussi delle applicazioni, applicazione di policy di segmentazione granulari e operazioni integrate di rilevamento e risposta alle violazioni. Queste funzionalità sono fondamentali per prevenire la perdita di dati e i problemi di downtime che possono interrompere le attività di uno studio legale.

Gli studi legali che utilizzano Akamai Guardicore Segmentation possono comprendere meglio il proprio ambiente, proteggere le loro applicazioni di importanza critica e ridurre drasticamente l'impatto e i loro tempi di risposta in caso di violazioni. Inoltre, le funzionalità di segmentazione basate su software fornite dalla soluzione sono significativamente più economiche, meno dispendiose in termini di tempo, più flessibili ed efficaci rispetto a quelle di molte altre soluzioni di segmentazione, come i firewall tradizionali. Nel complesso, Akamai Guardicore Segmentation è una soluzione di sicurezza leader del settore, progettata per affrontare i problemi legati alla sicurezza dei moderni studi legali.

Scoprite come salvaguardare i preziosi dati dei vostri clienti. Ulteriori informazioni sono disponibili sul sito akamai.com/guardicore.