Akamai

WHITEPAPER

Sicherheit in der modernen Anwaltskanzlei

Schutz von kritischen Anwendungen und Kundendaten

Einführung

Rechtsexperten haben jeden Tag mit sensiblen Daten zu tun. Vor diesem Hintergrund investieren viele Unternehmen in fortschrittlichere Sicherheitskontrollen und konzentrieren ihre Bemühungen darauf, ihre IT-Systeme und -Prozesse im Rahmen des Zero-Trust-Konzepts zu gestalten, um ihre kritischen Anwendungen zu schützen und den Zugriff durch Endnutzer zu kontrollieren.

Der Zero-Trust-Ansatz implementiert das Modell der geringsten Zugriffsrechte. Dieses Modell stellt sicher, dass autorisierte Nutzer, Systeme und Anwendungen nur den für ihre jeweilige Funktion nötigen Zugriff erhalten, und schützt gleichzeitig vor lateraler Netzwerkbewegung, Ransomware und unbefugtem Zugriff. Eine der flexibelsten und sichersten Methoden zur Implementierung des Zero-Trust-Ansatzes ist die Verwendung von Mikrosegmentierung.

Um zu verstehen, warum dies wichtig ist, sehen wir uns zunächst die Vergangenheit an.

Aufsehenerregende Angriffe: Ein Weckruf für die Rechtsbranche

Seit Jahren warnen die US-Bundesbehörden davor, dass große Rechtsunternehmen ein leichtes Ziel für Cyberkriminelle darstellen, da es dort datenreiche Repositorys mit Unternehmensdaten gibt. Das FBI warnte prominente Anwaltskanzleien bereits 2009 vor Angriffen durch organisierte Cyberkriminelle. Im Jahr 2011 luden sie sogar 200 der größten Anwaltskanzleien zu einem Gespräch über die Zunahme komplexer Cyberangriffe auf den Sektor ein.

> **Eine der flexibelsten und sichersten Methoden zur Implementierung des Zero-Trust-Ansatzes ist die Verwendung von Mikrosegmentierung.**

Seit 2014 haben laut Law.com mehr als 100 Anwaltskanzleien in 14 US-Bundesstaaten Datendiebstähle gemeldet. Der Legal Technology Survey Report, eine jährliche Umfrage der American Bar Association zur Nutzung von Technologie in der Rechtsbranche, ergab im Jahr 2022, dass mehr als ein Viertel der Anwaltskanzleien (jeder Größe) einem Angriff zum Opfer gefallen ist. Die Auswirkungen der Angriffe reichen von Ausfallzeiten aufgrund von Ransomware bis hin zu langwierigen Rechtsstreitigkeiten, nachdem Kundendaten im Internet veröffentlicht wurden.

Im Jahr 2015 erschien der Rechtssektor zum ersten Mal in der jährlichen Rangliste von Cisco der von Hackern angegriffenen Branchen. Infolgedessen forderten viele Finanzinstitute bei der Zusammenarbeit mit Anwaltskanzleien regelmäßige Prüfungen ihrer Cybersicherheitspraktiken.

Insbesondere zwei massive Angriffe auf die internationalen Anwaltskanzleien Mossack Fonseca & Co und DLA Piper gelten als Weckruf für die gesamte Rechts- und Finanzbranche. Über ein Leck, das den Namen „Panama Papers“ erhalten hatte, wurden mehr als 11 Millionen Dokumente mit Aufzeichnungen aus mehr als vier Jahrzehnten von der Offshore-Anwaltskanzlei Mossack Fonseca & Co gestohlen. Durch den Angriff wurden Steuerparadiese und Offshore-Konten globaler Unternehmen und einflussreicher Weltmarktführer aufgedeckt, was schwerwiegende Folgen hatte. Im Jahr 2018 gab das Unternehmen seine Schließung bekannt, was vor allem auf die Folgen des Angriffs zurückzuführen war. Anwaltskanzleien tragen die ethische und treuhänderische Verantwortung, alle angemessenen Anstrengungen zu unternehmen, um die ihnen anvertrauten Informationen zu schützen. Das Datenleck „Panama Papers“ stellt den bisher größten Angriff auf das Vertrauen zwischen einer Anwaltskanzlei und ihren Mandanten dar und hat zu einem Wandel im Cybersicherheitskonzept der Branche beigetragen. Doch trotz des neuen Schwerpunkts auf die Verbesserung der Sicherheitsvorkehrungen lassen sich Angreifer nicht abwimmeln.

> **Mehr als jede 4. Anwaltskanzlei hat bereits einen Angriff erlebt.**
>
> **– American Bar Association Legal Technology Survey Report 2022**

DLA Piper, eine der weltweit bekanntesten Anwaltskanzleien mit Niederlassungen in mehr als 40 Ländern, wurde fast zeitgleich mit Mossack Fonseca & Co zum Opfer eines NotPetya-Malware-Angriffs. Dies kostete das Unternehmen wochenlange Unterbrechungen, Geschäftseinbußen in Millionenhöhe, Wiederherstellungskosten und eine sehr schlechte Publicity.

In der jüngeren Vergangenheit verlor die Kanzlei Grubman Shire Meiselas & Sacks nach einem Ransomware-Angriff 756 Gigabyte an Daten über ihre prominente Kundschaft, zu der auch Lady Gaga, LeBron James und Madonna gehören. Da die Anwaltskanzlei nicht bereit war, das Lösegeld zu zahlen, gaben die Angreifer Informationen über Lady Gaga preis und versteigerten Daten, die angeblich Details über andere Kunden enthielten.

Moderne Anwaltskanzleien: Zeit für moderne Cybersicherheitslösungen

Die meisten der genannten Angriffe waren APT-Angriffe (Advanced Persistent Threat), die Phishing, Malware und Ransomware umfassten, und deren Zweck es war, sensible Kundendaten, Fusionsmaterialien, geistiges Eigentum und Finanzdaten zu stehlen. Mit Aussicht auf das große Vermögen werden Angreifer zunehmend von organisierten Verbrecherbanden unterstützt, die erhebliche Investitionen in Angriffstools und professionelle Teams tätigen.

> **Unternehmen ohne angemessene Segmentierung in ihrer IT-Umgebung riskieren im Falle eines Datendiebstahls den Verlust des Versicherungsschutzes.**

Bei der Entscheidung für oder gegen eine Anwaltskanzlei ist für immer mehr Mandanten Cybersicherheit ein entscheidender Faktor. Unternehmen ohne moderne Sicherheitskontrollen werden mit höherer Wahrscheinlichkeit Aufträge an Unternehmen verlieren, die Maßnahmen zur Verbesserung ihrer Sicherheit ergriffen haben und ihr Engagement für den Schutz von Kundendaten zeigen. Außerdem verlangen viele Cyberversicherungen jetzt eine Form der Segmentierung für sensible Daten und Anwendungen. Unternehmen ohne angemessene Segmentierung in ihrer IT-Umgebung riskieren im Falle eines Datendiebstahls den Verlust des Versicherungsschutzes.

Was fehlt: Schutz der kritischen Anwendungen des Unternehmens

Wie Sie sehen, sind vertrauliche Informationen in Kanzleien nicht mehr so sicher, wie sie einmal waren. Für Cyberkriminelle sind Anwaltskanzleien heute Tresore mit sensiblen Unternehmensdaten, die optimale Ziele für Cybersicherheitsangriffe darstellen.

Tatsächlich werden Anwaltskanzleien oft als einfacheres Ziel wahrgenommen als die meisten ihrer Mandanten. Aus diesem Grund wird ein Angreifer, der es auf bestimmte Daten eines Unternehmens abgesehen hat, häufig versuchen, über dessen Anwaltskanzlei an diese Daten zu kommen. Der sensible Charakter und die Vielfalt der von Anwaltskanzleien verwahrten Informationen in Verbindung mit deren allgemein schwächeren Sicherheitskontrollen machen sie zu einem lukrativen Ziel für Angreifer.

Angreifer sind sehr an den Informationen interessiert, die in den geschäftskritischen Anwendungen der Anwaltskanzlei gespeichert sind, insbesondere im Dokumentenmanagementsystem (DMS) und den E-Mails. Aus Sicht der IT-Sicherheit sind die wichtigsten Geschäftsanwendungen einer Anwaltskanzlei ihre DMS- und E-Mail-Anwendungen. Diese Anwendungen enthalten den Großteil der streng vertraulichen und sensiblen Mandantendaten und befinden sich in vielen Fällen nicht mehr nur in Rechenzentren vor Ort.

DMS-Anwendungen bieten zahlreiche Funktionen, darunter eine zentralisierte Organisation von Dateien und Ordnern, Versionsverwaltung, E-Mail-Verwaltung, Dokumentenbearbeitung, Indizierung und Suche, Berechtigungsverwaltung und mehr. Sie werden häufig in heterogenen IT-Umgebungen mit einer Mischung aus virtuellen und Bare-Metal-Servern eingesetzt und erfordern die Integration in mehrere andere Systeme mit unterschiedlichen internen Sicherheitsstufen. Mit diesen Integrationen kann eine Anwaltskanzlei zwar noch mehr von einem DMS profitieren, allerdings steigt dadurch auch das Risiko und die Angriffsfläche.

Die Endpunkte sind inzwischen so mobil und dynamisch, dass herkömmliche Sicherheitslösungen sie oft nicht schützen können, da sich Anwaltskanzleien wie viele andere Unternehmen vor allem auf die äußeren Grenzen des Netzwerks konzentrieren. Diese Lösungen bieten nicht mehr den Schutz, den Anwaltskanzleien für die Sicherung kritischer Anwendungen benötigen. Darüber hinaus fehlt es vielen Anwaltskanzleien noch an den nötigen Kontrollen, um Angreifer zu erkennen oder zu verhindern, dass Angriffe sich lateral ausbreiten und Zugriff auf sensible Datensysteme ermöglichen, sobald ein Angreifer über einen kompromittierten Endpunkt auf das Netzwerk zugreift.

Angesichts all dieser Herausforderungen investieren mittlerweile viele moderne Anwaltskanzleien in eine neue Generation von Cybersicherheitslösungen, die ihren einzigartigen und sich verändernden Anforderungen gerecht werden kann. Die softwarebasierte Segmentierung, insbesondere die Mikrosegmentierung, unterstützt einen Zero-Trust-Ansatz zur Sicherung kritischer Anwendungen und Daten, denn zur Steuerung der Kommunikation innerhalb des Netzwerks wird ein detaillierterer Ansatz bereitgestellt. So können nur autorisierte Nutzer und Systeme mit wichtigen Anwendungen kommunizieren. Dadurch wird es für einen Angreifer viel schwieriger, sich in Ihrem Netzwerk lateral zu bewegen, wodurch der Umfang eines potenziellen Angriffs begrenzt wird.

COVID-19 hat die Lage noch verschlimmert:

- Viele Anwaltskanzleien sind auf Remotearbeit umgestiegen
- Aus diesem Grund sind die Mitarbeiter nicht mehr in ihrer Niederlassung mit dem Netzwerk verbunden, sondern von unsicheren Heimnetzwerken aus
- Durch die vermehrte Nutzung von VPN- und VDI-Lösungen ist die Implementierung von Sicherheitsrichtlinien und die Zuordnung von Netzwerk-Traffic zu autorisierten Nutzern noch schwieriger

Vier Arten, wie Anwaltskanzleien Mandantendaten mit Akamai schützen können

Vollständige Transparenz

Umfassende Einblicke in Workloads, um alle offenen Verbindungen zu Anwendungen zu verstehen, in denen sensible Daten gespeichert sind.

Nutzerzugriffskontrolle

Implementieren Sie Richtlinien, die den Zugriff auf Anwendungen und Daten steuern, unabhängig davon, ob sie lokal oder in der Cloud gespeichert sind.

Softwarebasierte Segmentierung

Schnelle und flexible Mikrosegmentierung kritischer Anwendungen wie DMS und E-Mails, um die Exposition im Falle eines Angriffs zu begrenzen.

Bedrohungserkennung und -abwehr

Kombinieren Sie dynamische Segmentierungs- und Täuschungsfunktionen, um aktive Angriffe zu erkennen und einzudämmen und Mandantendaten zu schützen.

Einheitlicher Schutz mit Akamai Guardicore Segmentation

Akamai Guardicore Segmentation ist die branchenweit umfassendste Mikrosegmentierungslösung zum Schutz geschäftskritischer Anwendungen. Sie beschleunigt die Implementierung von Segmentierungsrichtlinien drastisch, vereinfacht die Wartung und ist auch effektiver bei der Abwehr von Bedrohungen, die auf laterale Netzwerkbewegungen angewiesen sind, um erfolgreich zu sein.

> **Um Mandantendaten besser zu schützen, nutzen viele Anwaltskanzleien Lösungen wie Mikrosegmentierung, um einen detaillierteren Ansatz zur Steuerung der Kommunikation innerhalb des Netzwerks zu implementieren, sodass nur autorisierte Nutzer und Systeme mit kritischen Anwendungen kommunizieren können.**

Unsere Lösung bietet eine visuelle Übersicht aller Anwendungen und anderen Assets in Ihrem Rechenzentrum, zusammen mit deren Abhängigkeiten voneinander. Sicherheitsbetreiber können dann schnell und intuitiv Sicherheitsrichtlinien auf Netzwerk- und Prozessebene erstellen und durchsetzen, um ihre kritischen Anwendungen und Assets zu isolieren und zu segmentieren. Dieser softwaredefinierte Segmentierungsansatz ist unabhängig von der zugrunde liegenden Infrastruktur, sodass Workloads, die sich auf Systemen vor Ort (sowohl ältere als auch moderne Systeme), VMs, Container, Clouds und Geräte erstrecken, konsistent geschützt werden können.

Richtlinien können für einzelne oder logisch gruppierte Anwendungen erstellt werden, unabhängig davon, wo im Rechenzentrum sie sich befinden. Diese Richtlinien geben vor, welche Anwendungen miteinander kommunizieren können und welche nicht und unterstützen so einen Zero-Trust-Ansatz. Eine weitere wichtige Funktion, die nur Akamai Guardicore Segmentation bietet, ist unsere integrierte Angriffserkennung und -reaktion, die die Komplexität der Verwaltung mehrerer dedizierter Tools reduziert. Die Erkennung von Angriffen und die Reaktion darauf sind erforderlich, um Vorschriften des New York State Department of Financial Services (DFS), anderer Auflagen an die Branche wie PCI DSS und zunehmend auch von hochkarätigen Kunden, die ihre Anwaltskanzleien prüfen, einzuhalten.

Akamai Guardicore Segmentation: Umfassender Schutz von kritischen Anwendungen

Schutz von Mandantendaten: Schaffen Sie die Grundlage für ein Zero-Trust-Framework, und setzen Sie in immer komplexeren und miteinander verbundenen Umgebungen IT-Hygiene und Best Practices durch.

Isolieren Sie kritische Anwendungen vom Rest der IT-Infrastruktur: Segmentieren Sie wertvolle Ressourcen wie DMS- oder E-Mail-Anwendungen mit Ringfencing-Richtlinien, um das Risiko von Bedrohungen innerhalb und außerhalb einer Anwaltskanzlei zu verringern.

Sichere und schnelle Einführung der Cloud: Ordnen Sie Workloads zu, und führen Sie vor der Migration eine Bestandsaufnahme aller kritischen Anwendungen und ihrer Abhängigkeiten durch. Ringfencing-Richtlinien nutzen diese Zuordnungen als Grundlage für eine konsistente Sicherheit, die Workloads während des gesamten Migrationsprozesses begleitet. Mit diesem Ansatz können Workloads schneller und sicherer in die Cloud migriert werden, wobei dieselben Sicherheitskontrollen beibehalten werden.

Sicherstellung der Geschäftskontinuität durch effiziente Angriffsabwehr: Nutzen Sie detaillierte Einblicke in den Ost-West-Traffic und Indikatoren für Angriffe, die auf ungewöhnliche Bewegungen hinweisen, um Cyberkriminelle aufzuhalten, bevor Ransomware oder eine andere Bedrohung das Geschäft zum Erliegen bringt.

Risikominderung durch Begrenzung der lateralen Netzwerkbewegung: Setzen Sie interne Grenzen und legen sie für geschäftskritische Anwendungen und Systeme Ringfence-Richtlinien fest, um die Angriffsfläche zu reduzieren. Das schützt effektiv vor der lateralen Ausbreitung von Angriffen und begrenzt im Ernstfall Schäden.

Fazit

Mit Akamai Guardicore Segmentation können Anwaltskanzleien die offenen Verbindungen, die bei einem Angriff verwendet werden könnten, visualisieren und verstehen. Darüber hinaus können Unternehmen diese Verbindungen damit durch Mikrosegmentierung sichern.

Unsere Lösung bietet umfassende Sicherheit für die kritischen Anwendungen einer Anwaltskanzlei in hybriden IT-Umgebungen, die sich sowohl auf virtuellen als auch auf Bare-Metal-Maschinen befinden, und zwar vor Ort sowie in IaaS- oder PaaS-Systemen. Sie bietet Transparenz in Bezug auf Anwendungsabhängigkeiten und -abläufe, die Durchsetzung von detaillierten Segmentierungsrichtlinien sowie integrierte Erkennung von Angriffen und die Reaktion darauf. Diese Funktionen sind entscheidend, um Datenverluste und Ausfallzeiten zu verhindern, die die Geschäftstätigkeit einer Anwaltskanzlei beeinträchtigen könnten.

Anwaltskanzleien, die Akamai Guardicore Segmentation verwenden, können ihre Umgebung besser verstehen, ihre kritischen Anwendungen schützen und die Auswirkungen und die Reaktionszeit im Falle eines Angriffs drastisch reduzieren. Darüber hinaus sind die bereitgestellten softwarebasierten Segmentierungsfunktionen wesentlich kostengünstiger, weniger zeitaufwendig, flexibler und effektiver als die Funktionen vieler anderer Segmentierungslösungen, wie etwa herkömmlicher Firewalls. Insgesamt ist Akamai Guardicore Segmentation eine branchenführende Sicherheitslösung, die gut für die Sicherheitsanforderungen moderner Anwaltskanzleien gerüstet ist.

Erfahren Sie, wie Sie die wertvollen Daten Ihrer Mandanten schützen. Erfahren Sie mehr über uns auf akamai.com/guardicore.