WHITEPAPER

Machen Sie Compliance mit Akamai Security zu einem Wettbewerbsvorteil

Ein auf vier Grundpfeilern basierender Ansatz zur Steigerung der Sicherheit und zur Vorbereitung auf Audits

Konzentrieren Sie sich auf vier Grundpfeiler der Sicherheit, um den Weg zur Compliance zu ebnen

Heutzutage müssen sich Unternehmen auf der ganzen Welt in einem immer schwierigeren Labyrinth von Vorschriften zurechtfinden – von der DSGVO über HIPAA bis hin zu PCI DSS und einer wachsenden Anzahl von regionalen Vorschriften. Doch Compliance-Bereitschaft zu zeigen, bedeutet nicht nur, Aufsichtsbehörden zufriedenzustellen – sie wird zu einem wichtigen Faktor, um das Vertrauen von Kunden und internen Stakeholdern wie Führungskräften und Vorstand aufrechtzuerhalten.

Die Auswirkungen von Compliance-Verstößen gehen sogar weit über direkte regulatorische Sanktionen hinaus. Zu den Kosten der Nichteinhaltung gehören Geschäftsunterbrechungen während der Ermittlungs- und Abhilfemaßnahmen, Reputationsschäden und erhöhte rechtliche Risiken. Wenn Unternehmen gegen Compliance-Anforderungen verstoßen, kann dies zu Umsatzeinbußen durch Kundenabwanderung führen und erhebliche operative Kosten verursachen, da Ressourcen in Abhilfemaßnahmen und nicht in Innovationen fließen. Laut Forrester hatten die 35 größten Compliance-Vergehen im Jahr 2024 weltweit Bußgelder in Höhe von 3 Milliarden US-Dollar zur Folge. In 23 Fällen waren dabei Verstöße gegen die Datenschutzgrundverordnung (DSGVO) der Europäischen Union ursächlich.

In der Vergangenheit war Compliance für Sicherheitsteams oftmals erst bei der Einführung von neuen Vorschriften ein Thema. Doch angesichts der rasanten Entwicklung der Technologie und immer komplexerer und intensiverer Angriffe muss das Thema Compliance bereits bei der Bewertung von Tools und Reifegradmodellen erörtert werden. Teams sollten sich folgende Fragen stellen: „Wie werden meine Sicherheitsentscheidungen von heute mich dabei unterstützen, die Compliance-Anforderungen jetzt und in Zukunft zu erfüllen?“

Bei Akamai helfen wir Kunden, diese Frage zu beantworten, indem wir uns bezüglich der Best Practices für die Sicherheit auf vier Grundpfeiler konzentrieren, die wie von selbst wichtige Elemente der Compliance-Bereitschaft fördern. Diese Grundpfeiler sind:

- Transparenz in der gesamten IT-Umgebung
- Verhindern von lateralen Bewegungen (in Netzwerken, Anwendungen und APIs)
- Verhindern von unbefugtem Zugriff
- Schutz von sensiblen Daten und Kontoinformationen

Das Ergebnis ergibt einen klaren Wettbewerbsvorteil. Unternehmen sind nicht nur sicherer, sondern auch besser darauf vorbereitet, regulatorische Hürden zu überwinden. Durch bessere Sicherheit und Compliance können sie auch das Vertrauen der Kunden und der internen Führung gewinnen.

Grundpfeiler 1

Transparenz in der gesamten IT-Umgebung

Grundlage für Compliance-Bereitschaft ist die umfassende Transparenz über alle digitalen Assets hinweg. Unternehmen können nicht schützen, was sie nicht sehen können. Regulierungsbehörden verlangen zunehmend Nachweise für eine vollständige Inventarisierung der Assets, kontinuierliche Überwachung und ein Bedrohungsbewusstsein.

Es ist allerdings nicht so einfach. Eine aktuelle Studie von Forrester ergab, dass etwas mehr als die Hälfte (52 %) der Finanzunternehmen zustimmen/uneingeschränkt zustimmen, dass sie über keine vollständige Transparenz ihrer IT-Umgebung verfügen. Leider sind die Risiken bei Compliance-Verstößen hoch – und zwar branchenunabhängig. Die Zahl der Unternehmen, die mehr als 100.000 US-Dollar an Bußgeldern zahlen mussten, stieg zwischen 2023 und 2024 um fast 20 %.

Für viele Unternehmen besteht die Herausforderung in Bezug auf Transparenz in der Überwachung des Netzwerktraffics und der APIs. Im Folgenden finden Sie einige Vorschriften und Standards, die Transparenz in Bezug auf Risiken erforderlich machen:

- Der Payment Card Industry Data Security Standard (PCI DSS) enthält Leitlinien, mit denen sichergestellt werden soll, dass die Software eines Unternehmens die Funktionen externer Komponenten sicher nutzt, z. B. APIs, die Zahlungsdaten von einer mobilen App an das System einer Bank übertragen.
- Standards wie die ISO-Norm (International Organization for Standardization) IEC 27001 erfordern die Trennung von Daten und Datenverarbeitungseinrichtungen für den Fall, dass ein Angreifer das Netzwerk kompromittiert.
- Das Datenschutzgesetz der Volksrepublik China verlangt zuverlässige Sicherheitskontrollen, um den Zugriff auf personenbezogene Daten von Kunden über Technologien zu sichern, die sensible Daten über verschiedene IT-Systeme hinweg austauschen.

Viele Unternehmen verfügen über Tools oder Prozesse, die einige dieser Anforderungen erfüllen können. Mit der Ausweitung auf hybride Computing-Umgebungen und über verschiedene Regionen hinweg wird die Überwachung jedoch deutlich schwieriger. Das gilt insbesondere für APIs. Laut einer Studie von Akamai wissen nur 27 % der Sicherheitsexperten, die über vollständige API-Bestände verfügen, tatsächlich, welche ihrer APIs sensible Daten zurückgeben – im Vergleich zu bereits besorgniserregenden 40 % im Jahr 2023.

Letztendlich müssen Unternehmen zur Koordination ihrer Sicherheitsmaßnahmen wissen, wo sich ihre sensiblen Daten befinden und wer bzw. was darauf zugreift. Dies erfordert Transparenz in folgenden Bereichen:

- Welche Assets kommunizieren mit dem Netzwerk (mit Echtzeit- und Verlaufsansichten), einschließlich Layer-7-Prozessen und Edge-Traffic, sowohl für Hybrid-Cloud- als auch für On-Premise-Umgebungen
- API-Bestandsaufnahme, einschließlich Schatten- und Zombie-APIs, aus der hervorgeht, wo APIs in Traffic-Quellen und Code integriert sind
- Clientseitiges JavaScript, das mit Blick auf die neuesten PCI-DSS-Anforderungen besonders wichtig ist

Das Portfolio von Akamai kann Sicherheitsteams dabei unterstützen, die erforderliche Transparenz zu erhalten.

Akamai Guardicore Segmentation kann Assets identifizieren und visualisieren, die innerhalb des Netzwerks kommunizieren, einschließlich Layer-7-Prozess-, Hash- und Befehlszeilendetails. Außerdem bietet es einen Überblick über den Verlauf als Nachweis bei Compliance-Audits, dass die betroffenen Assets nicht kompromittiert wurden. North-South- und East-West-Traffic-Visualisierungen zeigen außerdem, wo Zugriffe erfolgen.

API Security bietet eine Echtzeit-Bestandsaufnahme der APIs, die Unternehmen für Compliance benötigen, und trägt dazu dabei, zu erkennen, wo und wann unverschlüsselte Daten durch APIs fließen können.

App & API Protector bietet Transparenz auf Anwendungsebene, einschließlich API-Bestandsaufnahme, Erkennung der Offenlegung vertraulicher Daten und Echtzeit-Traffic-Analyse.

Client-Side Protection and Compliance bietet Transparenz bezüglich clientseitigen Skripten, die von PCI DSS v4 benötigt werden.

Ein Gesundheitsdienstleister implementierte Akamai Guardicore Segmentation, um HIPAA- und SOC 2-Compliance-Anforderungen zu erfüllen. Die Lösung lieferte wertvolle Einblicke in den Traffic zwischen verschiedenen Anwendungen. Das Sicherheitsteam konnte über die Layer-4-Protokolle hinaus detaillierte Daten untersuchen: Nutzer-IDs, Befehlszeileneingaben und sogar Dienstkorrelationen.

Grundpfeiler 2

Laterale Netzwerkbewegung verhindern

Genau wie Sicherheitsteams akzeptieren viele Aufsichtsbehörden, dass es selbst bei guter Sicherheitslage zu Verstößen kommen kann, und sie möchten sich vergewissern, dass Unternehmen den Schaden begrenzen können, der bei solchen Vorfällen entsteht. Beispiel:

- Artikel 32 der DSGVO erfordert „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“ sowie „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“.
- PCI DSS v4 verlangt von Unternehmen in ähnlicher Weise die „Einführung von Firewalls zum Schutz der Daten von Kreditkarteninhabern und die Gewährleistung, dass die Firewalls so konfiguriert sind, dass Verbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken eingeschränkt werden“.
- Die **Internationale Organisation für Normung/International Electrotechnical Commission (ISO/IEC) 27001** verlangt die Trennung von Daten und Datenverarbeitungseinrichtungen, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen

Während die meisten Unternehmen über eine Firewall verfügen, erfordert die Begrenzung von lateralen Bewegungen nach dem Eindringen von Schadakteuren in ein Netzwerk ein höheres Maß an Kontrolle. Dies macht die – vorzugsweise softwaredefinierte – Mikrosegmentierung zu einem wichtigen Werkzeug bei der Erreichung von Compliance. Akamai ist bestens positioniert, um den Bedenken von Auditoren hinsichtlich lateraler Bewegungen zu begegnen.

Akamai Guardicore Segmentation bietet die erforderliche Begrenzung lateraler Bewegungen für Unternehmen und ermöglicht so die Gewährleistung von Compliance. Vordefinierte Richtlinienvorlagen erleichtern die schnelle Durchsetzung von Compliance-Initiativen mit granularen Layer-7-Kontrollen. Und da es softwaredefiniert ist, kann es unabhängig vom Standort der Assets denselben granularen Schutz bieten. Darüber bewirkt die Möglichkeit zur Erkennung von Anwendungen, die innerhalb des Netzwerks kommunizieren, sowie von Kommunikationsversuchen zwischen segmentierten Zonen, dass das Vertrauen seitens der Auditoren in Ihre Fähigkeiten zur Abwehr von Bedrohungen weiter gestärkt wird.

Angreifer finden dank der zunehmenden Anzahl von APIs neue Möglichkeiten für laterale Bewegungen – insbesondere an API-Endpunkten, die anfällig für BOLA-Angriffe (Broken Object Level Authorization, fehlerhafte Autorisierung auf Objektebene) sind. Bedrohungsakteure können Objekt-IDs in API-Anfragen manipulieren, um eine laterale Bewegung im Netzwerk zu ermöglichen. Sobald sie eingedrungen sind, können Bedrohungsakteure die Autorisierung umgehen, Berechtigungen eskalieren und Zugriff auf Kundendaten erhalten.

Akamai API Security kann APIs markieren, die ohne ordnungsgemäße Authentifizierung sensible Daten offenlegen. Außerdem kann es APIs mit schwacher oder falsch konfigurierter Zugriffskontrolle – die unbefugten Datenzugriff und laterale Bewegungen zur Folge haben kann – identifizieren. Durch die Integration mit der Web Application Firewall (WAF) von Akamai kann API Security auch schädliche Bedrohungen in Echtzeit blockieren.

Ein Kunde von Akamai, ein weltweit tätiges Finanzdienstleistungsunternehmen, hatte mit unbekannten APIs in seiner Umgebung zu kämpfen und sich deswegen für die Implementierung von API Security entschieden. Die Bereitstellung hat die API-Verbreitung drastisch reduziert und die Compliance verbessert, da Akamai API Security sensible Daten klassifiziert, um Vorschriften wie die DSGVO, HIPAA und andere zu erfüllen. Im Rahmen von regulatorischen Audits dienen diese Umsetzungen als direkter Nachweis dafür, dass das Unternehmen geeignete technische Maßnahmen ergriffen hat.

Die heutigen KI-Bedrohungen sind die regulatorischen Hürden von morgen

Bei einer Untersuchung der Cybersicherheitsmaßnahmen eines Unternehmens darf heutzutage das Thema KI nicht außer Acht gelassen werden. Die schnelle Verbreitung von KI-basierten Anwendungen, großen Sprachmodellen und mit generativer KI verknüpften APIs führt zu neuen Schwachstellen, die vielen Unternehmen noch gar nicht bewusst sind. Beispiele für diese Arten von Anwendungen sind KI-gestützte Chatbots, Empfehlungs-Engines für den Einzelhandel, Tools für die Gesundheitsdiagnose und Engines für risikobasierte Entscheidungsfindung. Gleichzeitig setzen Bedrohungsakteure auf KI, um raffiniertere Angriffe zu starten.

Und überall dort, wo Bedrohungen für den Geschäftsbetrieb und die Öffentlichkeit entstehen, ist mit neuen Vorschriften zu rechnen.

Unternehmen, die ihre Investitionen in KI, ihre Daten und ihre Kunden schützen möchten, wenden sich an Akamai. Als Sicherheitsanbieter mit einer ausgewiesenen Erfolgsbilanz bei der Erfüllung heutiger Anforderungen in Bezug auf Transparenz, laterale Bewegungen und Zugriffskontrolle hat Akamai proaktiv in die Erfüllung der in Bezug auf KI zu erwartenden Anforderungen investiert. Akamai hat fortschrittliche KI-Funktionen entwickelt, um seine Sicherheitslösungen zu stärken, und hat nun eine Lösung eingeführt, mit der Unternehmen ihre eigenen KI-Investitionen schützen können.

Akamai Firewall for AI bietet umfassende Sicherheit für KI-gesteuerte Anwendungen, indem KI-spezifische Bedrohungen und Angriffe identifiziert und abgemildert werden, für die herkömmliche Sicherheitstools nicht gewappnet sind. Zu den spezifischen Schutzfunktionen von Firewall for KI gehören:

- **Prompt-Injection-Abwehr**: schützt vor Angreifern, die KI-Modelle durch betrügerische Eingaben manipulieren.
- **DLP (Data Loss Prevention, Schutz vor Datenverlust)**: erkennt und blockiert sensible Datenlecks in KI-generierten Antworten und schützt vor dem Empfang vertraulicher Daten in den Anfragen.
- **Filterung toxischer und schädlicher Inhalte**: kennzeichnet Hassrede, Fehlinformationen und anstößige Inhalte vor der Ausgabe.
- **Sicherheit der KI vor Angreifern**: schützt vor Remote-Code-Ausführung, Modell-Backdoors und Data Poisoning.
- **Denial-of-Service-Abwehr**: wehrt KI-gesteuerte DoS-Angriffe ab, indem übermäßige Abfrageauslastung und Modellüberlastung kontrolliert werden.

Darüber hinaus kann Firewall for AI Unternehmen dabei unterstützen, Datenschutz- und Sicherheitsrichtlinien einzuhalten. Durch die Durchsetzung KI-spezifischer Sicherheitsrichtlinien können Unternehmen Risiken im Zusammenhang mit Datenschutzvorschriften, ethischer KI-Nutzung und Corporate-Governance-Vorgaben mindern.

Grundpfeiler 3

Verhindern von unbefugtem Zugriff

Die Kontrolle des Zugriffs auf sensible Systeme und Daten stellt einen Grundpfeiler der Compliance über praktisch alle regulatorischen Rahmenbedingungen hinweg dar. Unternehmen müssen ihre Anwendungs- und API-Sicherheitslage verstehen und unbefugten Zugriff und Missbrauch verhindern. Dies erfordert eine angemessene Authentifizierung der Nutzer, die Autorisierung des Zugriffs auf einer „Need-to-Know"-Basis und die detaillierte Aufzeichnung aller Zugriffsaktivitäten.

Für eine vollständige Zugriffskontrolle, die die gesetzlichen Anforderungen erfüllt, müssen Unternehmen drei wichtige Herausforderungen bewältigen. Das Sicherheitsportfolio von Akamai kann dazu beitragen, umfassende Abwehrmechanismen zu bieten, die sich mit den folgenden Aspekten befassen:

1. **Umfassendes Verständnis der Sicherheitslage von Anwendungen und APIs**

App & API Protector von Akamai ermöglicht Unternehmen, Traffic-Richtlinien in allen Umgebungen durchsetzen, in denen sie ausgeführt werden, während Akamai API Security Unternehmen auf ungewöhnliche Aktivitäten und unbefugte Datenzugriffe oder fehlerhafte Konfigurationen aufmerksam machen kann. All dies sind wichtige Aspekte für Auditoren. Unterdessen kann Akamai Guardicore Segmentation alle Anwendungen verfolgen, die innerhalb des Netzwerks kommunizieren, und eine Baseline für Aktivitäten festlegen.

2. **Überwachen Sie das Nutzerverhalten und beschränken Sie den Zugriff auf vertrauliche Informationen**

Akamai Guardicore Segmentation begrenzt den Zugriff innerhalb des Netzwerks anhand der Identität des Nutzers, während **App & API Protector** Traffic-Richtlinien mit KI-basierter Bedrohungserkennung durchsetzt, um Sicherheitsverstöße zu verhindern. Und schließlich überwacht **Client-Side Protection & Compliance** das Ausführungsverhalten von JavaScript, um Client-seitige Angriffe abzuwehren.

3. **Betrügerische Aktivitäten erkennen und einschränken**

API Security trägt dazu bei, ungewöhnliches API-Verhalten und falsch konfigurierte Authentifizierungskontrollen zu erkennen, um Angriffe mit hohem Risiko zu blockieren. Akamai Guardicore Segmentation schützt das Netzwerk, indem es verdächtige Verbindungen markiert und blockiert, die ein Anzeichen für betrügerische Aktivitäten sein können. App & API Protector erkennt und wehrt Bedrohungen ab, die von OWASP identifiziert wurden, um das Betrugsrisiko weiter zu verringern.

NIS2 und Sicherung des Zugriffs

Die aktualisierte Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) soll einen gemeinsamen Cybersicherheitsstandard in allen EU-Mitgliedsstaaten schaffen. Seit neuestem umfasst NIS2 auch die Anforderung, dass Unternehmen ein Informationssicherheitsmanagement-System aufbauen müssen, das Personen, Richtlinien und Technologien bewertet, um sensible Daten zu schützen und die betriebliche Resilienz zu gewährleisten. NIS2 legt auch ein stärkeres Augenmerk auf die Sicherung von IT-Lieferketten und Beziehungen zu Drittanbietern.

Grundpfeiler 4

Schutz von sensiblen Daten und Kontoinformationen

Der letzte Grundpfeiler eines umfassenden Ansatzes zur Einhaltung gesetzlicher Vorschriften erfordert, dass Unternehmen über Pläne zum Umgang mit sensiblen Daten verfügen. Die Sicherung der Daten von Kunden, Patienten, Partnern und mehr ist das Herzstück der meisten sicherheitsorientierten Vorschriften.

Beispielsweise erfordert das japanische Gesetz zum Schutz personenbezogener Daten Datenschutzfolgeabschätzungen, die Risiken für Technologien erkennen und mindern können, welche große Mengen personenbezogener Daten verarbeiten oder hochriskante Datenverarbeitungsaktivitäten umfassen.

Für US-amerikanische Finanzinstitute verlangt der Federal Financial Institutions Examination Council (FFIEC) Kontrollen, die sicherstellen, dass APIs über mehrstufige Sicherheitsmaßnahmen nur den Zugriff auf bestimmte Daten für autorisierte Nutzer ermöglichen, z. B. durch Überwachung, Protokollierung und Berichterstellung.

Die Umsetzung dieses Grundpfeilers beginnt mit der Bedrohungserkennung. Die WAAP-Lösung (Web Application and API Protection) **App & API Protector** von Akamai bildet die erste Verteidigungsstufe, während **Akamai Guardicore Segmentation** sowohl den North-South- als auch den East-West-Traffic überwacht und segmentiert. Das **Bot Abuse & Protection-Lösungsportfolio** von Akamai bietet eine zusätzliche Sicherheitsebene zum Schutz vor automatisierten Bedrohungen und durch Menschen gesteuerte Angriffe.

Um Bedrohungen richtig zu erkennen, müssen Unternehmen jedoch auch das grundlegende Verhalten in ihrem Netzwerk verstehen. So können die Funktionen von Akamai Security diese wichtigen Erkenntnisse liefern:

- Akamai API Security und Akamai Guardicore Segmentation enthalten ein grundlegendes Verständnis von APIs und Apps, die innerhalb des Netzwerks kommunizieren, und können auf ungewöhnliches Verhalten hinweisen.
- Adaptive Security Engine – eine Schlüsseltechnologie von App & API Protector – verwendet lokale und globale Daten und erlernt so Angriffsmuster, um kundenspezifische Anpassungen von Schutzmaßnahmen vorzunehmen und so zukünftige Bedrohungen abzuwehren.
- Akamai Hunt, ein verwalteter Threat-Hunting-Service, der auf das Expertenteam von Akamai setzt, ermöglicht Unternehmen einen proaktiveren Verteidigungsansatz.

DORA und Datensicherheit

Der Digital Operational Resilience Act (DORA) der Europäischen Union soll Finanzdienstleister in EU-Mitgliedsstaaten dabei unterstützen, Cyberangriffe zu verhindern und sich von ihnen zu erholen. Mit DORA verfügt der Sektor über ein verbindliches, umfassendes Risikomanagement-Framework für die Informations- und Kommunikationstechnologie (IKT). Gemäß Artikel 3 von DORA müssen Unternehmen IKT-Lösungen und -Prozesse verwenden, die die folgenden Anforderungen erfüllen:

- Minimieren von datenbezogenen Risiken, unbefugtem Zugriff und technischen Mängeln
- Verhindern von Nichtverfügbarkeit von Daten, Datenverlusten sowie Verstößen gegen Integrität und Vertraulichkeit
- Gewährleistung der Datenübertragungssicherheit

Von isolierter Compliance zum Wettbewerbsvorteil

Effektive Compliance-Programme müssen geschäftlich relevant sein und dürfen gesetzliche Anforderungen nicht nur pro forma erfüllen. Unternehmen, die die Compliance-orientierten Sicherheitslösungen von Akamai implementieren, haben messbare Verbesserungen in drei wichtigen Dimensionen gemeldet.

Senkung der Compliance-Kosten

Unternehmen mit ausgereiften Compliance-Programmen geben in der Regel weniger für Compliance-Aktivitäten aus als Unternehmen, die einen Ad-hoc-Ansatz verfolgen. Die Automatisierung der Nachweiserfassung über integrierte Sicherheitsplattformen kann die Vorbereitungszeit für Audits erheblich verkürzen, ebenso wie die Konsolidierung von Punktlösungen auf einer umfassenden Plattform.

Verbesserung der Risikolage

Neben der Kostensenkung sollten Compliance-Verbesserungen zu einer messbaren Risikoreduzierung führen. Unternehmen, die die Segmentierungslösungen von Akamai implementieren, können für laterale Bewegungen anfällige Pfade einschränken, indem sie die wichtigsten Compliance-Anforderungen unmittelbar erfüllen und zugleich die Risiken für ihre Organisation reduzieren.

Umfassende Überwachungsfunktionen verbessern die Transparenz. Auf diese Weise werden Risiken unmittelbar reduziert, indem blinde Flecken beseitigt werden, an denen Compliance-Verstöße sonst nicht erkannt werden.

Betriebliche Effizienz

Die dritte Dimension der Compliance-Auswirkungen umfasst Verbesserungen bei der betrieblichen Effizienz. Vorab genehmigte Kontrollen und konsistente Sicherheitsmuster können zu deutlich schnelleren Sicherheitsgenehmigungen für neue Anwendungen führen. Dadurch wird die Zufriedenheit der Entwickler verbessert, indem die potenziellen Probleme bei den Sicherheitsüberprüfungsverfahren verringert und die Markteinführungszeit für neue Anwendungen verkürzt wird.

Feinabstimmung der Compliance

Da sich gesetzliche Auflagen ständig weiterentwickeln und Unternehmen wachsen, benötigen sie einen Compliance-Ansatz, der sich anpassen lässt. Das integrierte Sicherheitsportfolio von Akamai bildet die Grundlage für eine Compliance-Strategie, die regulatorische Trends antizipiert und an das Unternehmenswachstum angepasst werden kann.

- Konfigurierbare Richtlinien-Frameworks können an neue Anforderungen angepasst werden, ohne dass eine wesentliche Neugestaltung erforderlich ist, während erweiterbare Reporting-Funktionen mit neuen Nachweisanforderungen Schritt halten können, wenn Vorschriften weiterentwickelt werden.
- Die automatisierte Richtlinienbereitstellung für neue Assets stellt sicher, dass die Compliance-Abdeckung bei einer Vergrößerung des Unternehmens automatisch erweitert wird.
- Zentralisierte Verwaltungsfunktionen sorgen größenunabhängig für flächendeckende Transparenz, während eine umfassende API-Unterstützung die Automatisierung von Compliance-Prozessen ermöglicht, um die zunehmende Komplexität zu bewältigen.

Darüber hinaus müssen Unternehmen proaktiv vorgehen, um eine regelmäßige Überprüfung von Vorschriften und die entsprechende Aktualisierung ihrer Compliance-Kontrollen vorzunehmen. Die Sicherheitslösungen von Akamai werden regelmäßig aktualisiert und an die sich ständig ändernden Compliance-Anforderungen angepasst, sodass sichergestellt ist, dass Kunden diese dauerhaft erfüllen können.

Fazit: Compliance als Wettbewerbsvorteil

Bei effektiver Compliance geht es nicht mehr nur um die Erfüllung behördlicher Anforderungen, sondern es handelt sich um ein strategisches Geschäftsziel, das sich direkt auf die Unternehmensperformance, das Kundenvertrauen und die Wettbewerbsposition auswirkt. Unabhängig von Ihrer Branche oder Region sorgt ein proaktiver Compliance-Ansatz für eine robuste und agile Sicherheitslage.

Durch Implementierung eines integrierten Sicherheitsansatzes für die vier Grundpfeiler der Compliance-Bereitschaft – Transparenz in der gesamten IT-Umgebung, Schutz vor lateralen Netzwerkbewegungen, Verhindern von unbefugtem Zugriff und Schutz von sensiblen Daten und Kontoinformationen – können Unternehmen eine nachhaltige Compliance-Basis schaffen, die nicht nur die Erfüllung gesetzlicher Vorschriften ermöglicht, sondern darüber hinaus auch einen geschäftlichen Mehrwert bietet.

Die Unternehmen, die den größten Erfolg verzeichnen, sind diejenigen, die Compliance von den notwendigen Kosten für die Geschäftstätigkeit in einen strategischen Vorteil verwandelt haben, der die digitale Transformation ermöglicht und gleichzeitig das schützt, was am wichtigsten ist: Kundenvertrauen, Datenintegrität und Unternehmensreputation.

Kontaktieren Sie uns, um zu erfahren, wie Akamai Ihr Unternehmen unterstützen kann.

Kontakt