



Gesetzliche Compliance für Finanzdienstleistungen

5 wichtige Geschäftsziele



Inhaltsverzeichnis

Vereinfachen der Compliance	02
Steigern der Produktivität	03
Verbessern des Kundensupports	04
Effektives Verwalten der Sicherheits- und Compliance-Kosten	05
Ausfallsicherheit und Vertrauensaufbau	06
Globale Bank erreicht SWIFT-Compliance innerhalb von zwei Wochen	07
Fazit	08

Verbesserte Compliance-Funktionen bei Finanzdienstleistungen können zu besseren Kundenerlebnissen, höherer Produktivität und stabilerem Wachstum führen.

In der schnelllebigen Welt der Finanzdienstleistungen sind Compliance und betriebliche Ausfallsicherheit von entscheidender Bedeutung. Dieses E-Book enthält einen strukturierten Ansatz zur Vereinfachung der Compliance, zur Steigerung der Produktivität, zur Verbesserung des Kundenerlebnisses, zur effektiven Verwaltung der Sicherheitskosten sowie zur Schaffung von Ausfallsicherheit und Vertrauen. Compliance allein garantiert zwar keine vollständige Sicherheit, doch für Führungsteams bleibt sie eine oberste Priorität. Immerhin können nicht bestandene Audits zu Geschäftsunterbrechungen und erheblichen finanziellen Auswirkungen führen.

Compliance-Bewertungen sind für Sicherheitsteams bekanntermaßen zeitaufwändig und ressourcenintensiv. Der Wandel hin zu perimeterlosen digitalen Umgebungen und die Zunahme der Remote-Arbeit haben die Herausforderung nur noch weiter vergrößert. Finanzinstitute müssen ihre Umgebungen isolieren und regulierte Assets abgrenzen, um Standards wie den Payment Card Industry Data Security Standard (PCI DSS), das Gesetz über die digitale betriebliche Resilienz (Digital Operational Resilience Act, DORA) und das System der Society for Worldwide Interbank Financial Telecommunication (SWIFT) zu erfüllen. Dieses E-Book bietet Einblicke und Strategien, die ein Finanzinstitut dabei unterstützen, diese komplexen Herausforderungen zu meistern und die folgenden **5 wichtigen Geschäftsziele** zu erreichen:



Akamai für Finanzdienstleister

Heute vertrauen die größten Marken in den Bereichen Banking, Kapitalmärkte, Versicherungswesen und FinTech darauf, dass Akamai die Cloud von einem chaotischen Ort mit einer unvorhersehbaren Performance und versteckten Bedrohungen in eine sichere, zuverlässige und kostengünstige Umgebung für ihre Geschäfte verwandelt.

Zu unseren Kunden gehören:

alle **20** führenden Broker

17 der **20** führenden Banken

7 der führenden **10** FinTech-Unternehmen

1



Vereinfachen der Compliance

Durch die Unterteilung von Netzwerken in kleinere Perimeter und die Isolierung einzelner Workloads können Mikrosegmentierungslösungen den Umfang von Compliance-Umgebungen beschränken, Audits optimieren, den Zugriff auf vertrauliche Informationen einschränken und gleichzeitig einen unvergleichlichen Einblick in Netzwerktraffic und Datenflüsse bieten.

Reduzierter Umfang von Compliance-Umgebungen

Durch die Segmentierung Compliance-bezogener Daten aus anderen IT-Assets kann der Umfang der Compliance-Maßnahmen erheblich minimiert werden, was mit einer Reduzierung der Kosten und der Komplexität einhergeht. Finanzinstitute können ihre Compliance-Aktivitäten auf bestimmte Segmente des Netzwerks konzentrieren, wodurch der Prozess effizienter und weniger ressourcenintensiv wird.

Optimierte Compliance-Maßnahmen und Auditprozesse

Mikrosegmentierung vereinfacht die Einhaltung von Audit-Anforderungen und -Prozessen, indem der Umfang von Compliance-Umgebungen verringert wird und die Einhaltung von Vorschriften einfacher nachgewiesen werden kann. Dieser optimierte Ansatz spart nicht nur Zeit ein, sondern erhöht auch die Genauigkeit bei der Erfüllung der gesetzlichen Anforderungen.

Geschützte APIs

Durch die Implementierung von zuverlässigen API-Sicherheitsmaßnahmen, wie im neuesten Handbuch des Federal Financial Institutions Examination Council (FFIEC) zur Prüfung der Informationstechnologie beschrieben, können Finanzinstitute APIs und vertrauliche Daten sowie sich selbst besser vor Angriffen schützen. Dies ist entscheidend für die Einhaltung strenger API-Sicherheitsbestimmungen.



2



Steigern der Produktivität

Einheitliche Sicherheitsverwaltung

Die Konsolidierung der Sicherheitsverwaltung mit der einheitlichen Plattform von Akamai reduziert den Zeitaufwand für die Verwaltung mehrerer Sicherheitslösungen und verbessert die betriebliche Effizienz. Dieser Ansatz ermöglicht es Sicherheitsteams, sich auf strategische Initiativen statt auf operative Punktlösungen zu konzentrieren.

Proaktives Threat Hunting

Durch eine Verbesserung der Produktivität mit proaktivem Threat Hunting lassen sich Bedrohungen identifizieren und neutralisieren, bevor sie Einfluss auf den Betrieb haben können. Dies sorgt für eine gleichmäßigere Geschäftskontinuität. Die fortschrittlichen Funktionen zur Bedrohungserkennung und -abwehr von Akamai ermöglichen eine effiziente Ressourcenzuweisung.

Fortschrittlicher API-Schutz

Durch den Einsatz von Laufzeitschutzfunktionen auf der Grundlage von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) können Finanzinstitute fortschrittliche API-Angriffe in Echtzeit erkennen und blockieren, was raffiniert vorgehende Cyberkriminelle abwehrt und die Gesamtproduktivität steigert.



3



Verbessern des Kundensupports

Nahtloser Nutzerzugriff

Die Gewährleistung eines nahtlosen und sicheren Kundenerlebnisses mit den Edge-Sicherheitslösungen von Akamai schützt Nutzerdaten und sorgt für eine hohe Performance, unabhängig vom Standort des Nutzers. Die verbesserte Serviceverfügbarkeit durch DDoS-Schutz (Distributed Denial of Service) und Lastausgleich stellt einen kontinuierlichen Service sicher, der für die Wahrung des Kundenvertrauens und der Kundenzufriedenheit entscheidend ist.

Personalisierte Sicherheitsrichtlinien

Durch die Implementierung personalisierter Sicherheitsrichtlinien, die sich an das Verhalten und die Anforderungen der einzelnen Nutzer anpassen, wird das Kundenerlebnis insgesamt verbessert und gleichzeitig eine zuverlässige Sicherheit gewährleistet. Die Lösungen von Akamai stellen sicher, dass Finanzinstitute ihren Kunden ein sicheres und personalisiertes Erlebnis bieten können.

Echtzeit-API-Überwachung

Das Prüfen des API-Verhaltens mithilfe von Echtzeitanalysen ermöglicht Finanzinstituten, Bedrohungen schnell zu erkennen und darauf zu reagieren. So werden sensible Daten geschützt und ein reibungsloses und sicheres Kundenerlebnis gewährleistet.



4



Effektives Verwalten der Sicherheits- und Compliance-Kosten

Skalierbare Sicherheitslösungen

Die skalierbaren Sicherheitslösungen von Akamai passen sich Ihren Geschäftsanforderungen an und bieten kosteneffektiven Schutz, ohne dass Sie erhebliche Summen investieren müssen. Dank dieser Skalierbarkeit können Finanzinstitute ihre Sicherheits- und Compliance-Kosten effektiv verwalten.

Senkung der Betriebskosten

Durch den Einsatz der cloudbasierten Services von Akamai sind teure On-Premise-Infrastrukturen nicht mehr nötig. Das umfassende Risikomanagement-Framework von Akamai kann dazu beitragen, Risiken effizient zu identifizieren, zu bewerten und zu mindern, wodurch potenzielle finanzielle Verluste durch Sicherheitsverstöße reduziert werden können.

Vereinfachte Compliance-Audits

Durch die Reduzierung des Umfangs von Compliance-Umgebungen und die Vereinfachung von Compliance-Nachweisen simplifizieren die Mikrosegmentierungslösungen von Akamai den Audit-Prozess, sparen Zeit und senken die Gesamtkosten für das Compliance-Management.

Außerdem bieten sie die Flexibilität, die Finanzinstitute von heute benötigen, um schnell Schnittstellen zu optimieren, Visualisierungen nachzustimmen, Geschäftsregeln anzupassen und neue Informationen zu integrieren. Das Ergebnis ist eine viel umfassendere und wandlungsfähigere Lösung, die sich an die Anforderungen des Fallmanagements anpasst.



5



Ausfallsicherheit und Vertrauensaufbau

Verbesserte betriebliche Ausfallsicherheit

Ein hohes Niveau digitaler betrieblicher Ausfallsicherheit zu erreichen, ist für Finanzinstitute von entscheidender Bedeutung, um in der sich ständig weiterentwickelnden Bedrohungslandschaft zu bestehen. Die Lösungen von Akamai unterstützen Finanzinstitute dabei, Cybersicherheitsvorfälle zu verhindern, darauf zu reagieren und sich von diesen zu erholen. So wird ein kontinuierlicher Betrieb sichergestellt und das Vertrauen der Kunden gestärkt.

Zuverlässige Sicherheitsmaßnahmen

Weltweit betonen Regulatoren die Notwendigkeit zuverlässiger Cybersicherheitsmaßnahmen. Das umfassende Sicherheitsportfolio von Akamai ist auf diese gesetzlichen Anforderungen abgestimmt und stellt Finanzinstituten die Tools zur Verfügung, die für die Aufrechterhaltung der betrieblichen Ausfallsicherheit und den Schutz vor hoch entwickelten Bedrohungen erforderlich sind.

Vertrauen und Stabilität

Die Sicherheitslösungen von Akamai schützen nicht nur vor aktuellen Bedrohungen, sondern bilden auch eine Grundlage für Vertrauen und Stabilität. Durch die Integration von Sicherheit in den Kern ihrer Geschäftstätigkeit können Finanzinstitute einen langfristig stabilen Betrieb gewährleisten und das Vertrauen ihrer Kunden wahren.



Das Wichtigste ist, die eigene Angriffsfläche zu erfassen und dann in der Lage zu sein, sie zu kontrollieren. Ein Einblick in das, was in der Umgebung vor sich geht, ist ein wesentlicher Risikoindikator. Durch die Überwachung der Aktivitäten von Red Teams konnten wir schnell Richtlinien entwickeln, um häufige Angriffsvektoren zu blockieren.

– Chief Information Security Officer (CISO) eines registrierten Wertpapierbrokers/-händlers

Globale Bank erreicht SWIFT-Compliance innerhalb von zwei Wochen

Externe Aufsichtsbehörden verlangten von einem Kunden von Akamai, einer globalen Bank, alle wichtigen Anwendungen zu schützen, um die SWIFT-Anforderungen zu erfüllen. Diese beinhalten einen sicheren Prozess für Geldtransfers zwischen Finanzinstituten. In der Regel erfordert eine Anwendung wie diese mehr als 100 Server, die an verschiedenen Standorten bereitgestellt werden, einschließlich Bare-Metal- und virtueller Server. Im Durchschnitt würde dieser Prozess bei einer Bank dieser Größe mit Planung und Ausführung zwischen acht und zwölf Monate dauern, da ein Virtual Local Area Network (VLAN) für das Segment über mehrere Standorte hinweg erstellt werden müsste. Das Ermitteln der Abhängigkeiten der SWIFT-Anwendung und das Sicherstellen, dass der Regelsatz korrekt ist, hätte den Zeitplan nur verlängert.

Gleichzeitig hätte das Projekt auch den Kauf neuer Firewall-Anlagen erfordert. Da die SWIFT-Anwendung für das Bankgeschäft von entscheidender Bedeutung ist, kann die Bank sich keine Ausfallzeiten leisten. Alles in allem war damit zu rechnen, dass das Segmentierungsprojekt einen enormen Aufwand seitens einer Vielzahl von Mitarbeitern erfordern würde.

Doch mit Akamai brauchte ein einziger Security Engineer für den gesamten Prozess nur etwa zwei Wochen. Es waren keine Netzwerkänderungen erforderlich und die Bank konnte den Wechsel von Anwendungen und Ausfallzeiten vermeiden.

ZEITERSPARNIS

226–351 Tage

VZÄ-REDUZIERUNG

> 4 VZÄ

UND DAS ALLES

ohne Ausfallzeiten

UND MIT VERBESSERTER
TRANSPARENZ

Zeitersparnis und verbesserte Transparenz:

Ein Finanzinstitut musste seine SWIFT-Anwendung abschirmen, die sich innerhalb einer komplexen Umgebung mit Bare-Metal-, VMware- und OpenStack-Infrastruktur befand. Herkömmliche Segmentierungsmethoden erwiesen sich als schwierig, hätten acht bis zwölf Monate gedauert und mehr als fünf Vollzeitäquivalente (VZÄ) benötigt, was zusätzliche Probleme mit Ausfallzeiten und mangelnder Transparenz von Anwendungen und Abhängigkeiten mit sich gebracht hätte. Durch die Implementierung von Akamai Guardicore Segmentation konnte das Unternehmen die SWIFT-Anwendungszuordnung mit automatisch vorgeschlagenen und fein abgestimmten Segmentierungsrichtlinien innerhalb von Stunden abschließen. Es waren weder neue Hardware noch Firewalls erforderlich. Der gesamte Prozess wurde in zwei Wochen mit nur einem VZÄ abgeschlossen.

Fazit

Akamai bietet umfassende Lösungen, anhand derer sich Finanzinstitute in der komplexen Landschaft der gesetzlichen Compliance und der Cybersicherheit zurechtfinden. Durch den Einsatz fortschrittlicher Technologien wie Mikrosegmentierung können Finanzinstitute die Compliance vereinfachen, die Produktivität steigern, das Kundenerlebnis verbessern, die Kosten für Sicherheit und Compliance effektiv verwalten sowie Ausfallsicherheit und Vertrauen aufbauen. Dank der nachweislichen Erfolgsbilanz und der innovativen Lösungen von Akamai ist das Unternehmen ein idealer Partner für Finanzinstitute, die ihre Sicherheitslage stärken und die Einhaltung gesetzlicher Vorschriften gewährleisten möchten.

Erfahren Sie mehr über unsere Lösungen für Finanzdienstleister.

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Wir nutzen die Größe und Einblicke unserer globalen Plattform, um gemeinsam mit Ihnen Bedrohungen vorzubeugen, zu erkennen und abzuwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können.

