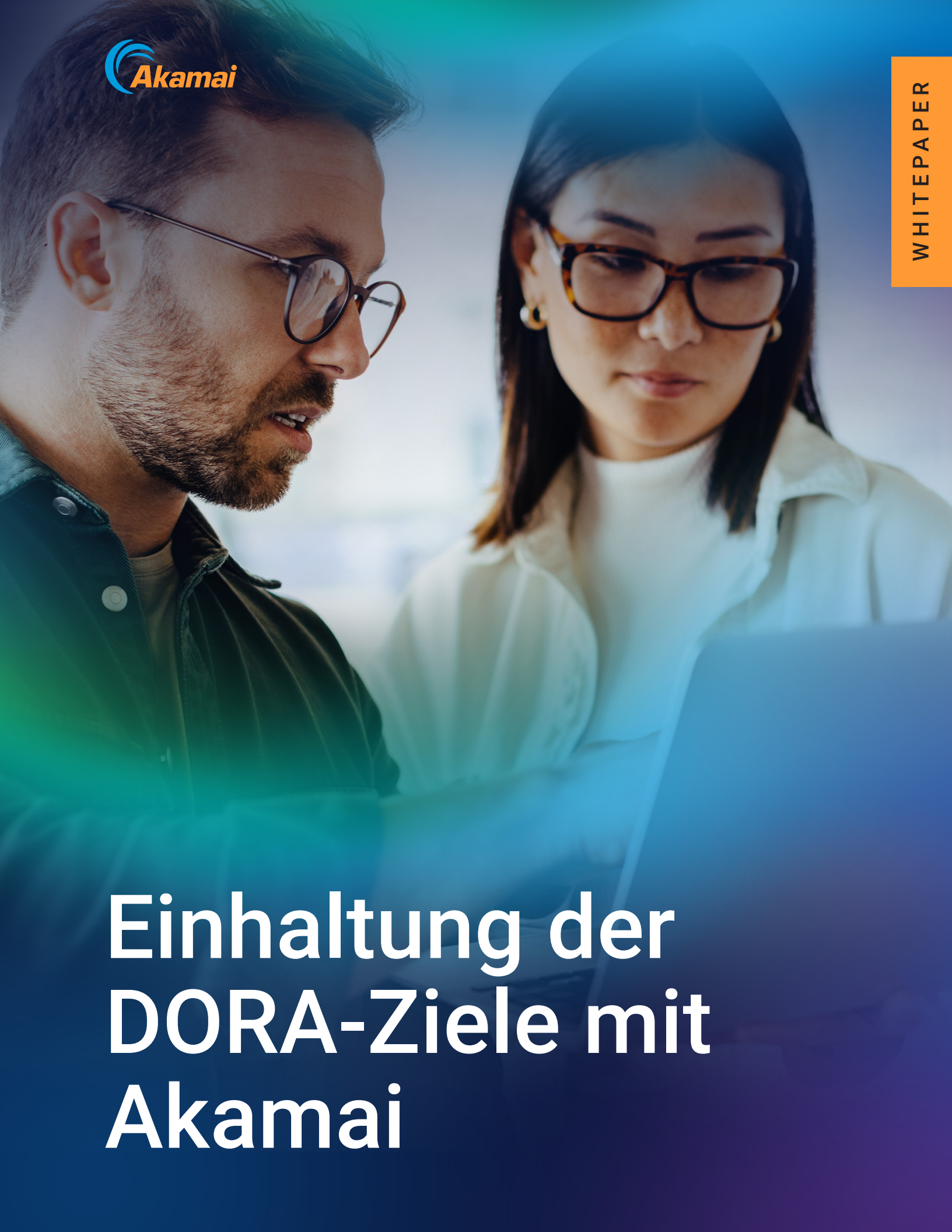


WHITEPAPER

Einhaltung der DORA-Ziele mit Akamai

Das Konzept der digitalen operationalen Resilienz hat sich im Laufe der Jahre insbesondere im Bereich der Finanzdienstleistungen erheblich weiterentwickelt. Anfänglich konzentrierten sich Finanzunternehmen auf Pläne zur Notfallwiederherstellung und Geschäftskontinuität. Diese frühen Bemühungen bestanden in erster Linie aus Reaktionen zur Wiederherstellung von Diensten nach einer Störung. Je häufiger und fortschrittlicher die Cyberbedrohungen wurden, desto stärker verlagerte sich der Fokus dann auf vorausschauende Maßnahmen. Finanzunternehmen begannen, zuverlässige Cybersicherheitsprotokolle, regelmäßige Systemaktualisierungen und Schulungsprogramme für Mitarbeitende einzuführen, um Störungen noch vor deren Auftreten zu verhindern. Mit dem Aufkommen fortschrittlicher Technologien wie Large Language Models (LLMs), künstliche Intelligenz (KI) und maschinelles Lernen (ML) wurde die Herangehensweise an operationale Resilienz revolutioniert. Diese Technologien haben jedoch auch die Bedrohungsvektoren revolutioniert, wodurch Bedrohungen komplexer und häufiger wurden. Daher muss sich die operationale Resilienz kontinuierlich an diese immer neuen Herausforderungen anpassen.

Dank dieser Technologien ist es möglich, prädiktive Analysen anzustellen, die Bedrohungserkennung zu automatisieren und die Reaktionszeiten zu verkürzen, was die Resilienz deutlich stärkt. Und mit zunehmender Kontrolle seitens der Behörden hat das Thema der digitalen operationalen Resilienz einen weiteren Schub erfahren. So haben Vorschriften wie die Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU) dazu beigetragen, die für den Datenschutz und die Betriebskontinuität geltenden Maßstäbe anzuheben. Die zunehmende Komplexität und Häufigkeit der Cyberbedrohungen sind jedoch die Hauptfaktoren, die Finanzunternehmen dazu bewegen, umfassendere Resilienzstrategien einzuführen. Moderne Ansätze für digitale operationale Resilienz sehen nun ein ganzheitliches Risikomanagement vor. Darunter fallen nicht nur technische Sicherheitsvorkehrungen, sondern auch Governance-Regelungen, der Umgang mit Drittparteienrisiken, kontinuierliche Überwachungs- und Verbesserungsmaßnahmen sowie der Informationsaustausch.

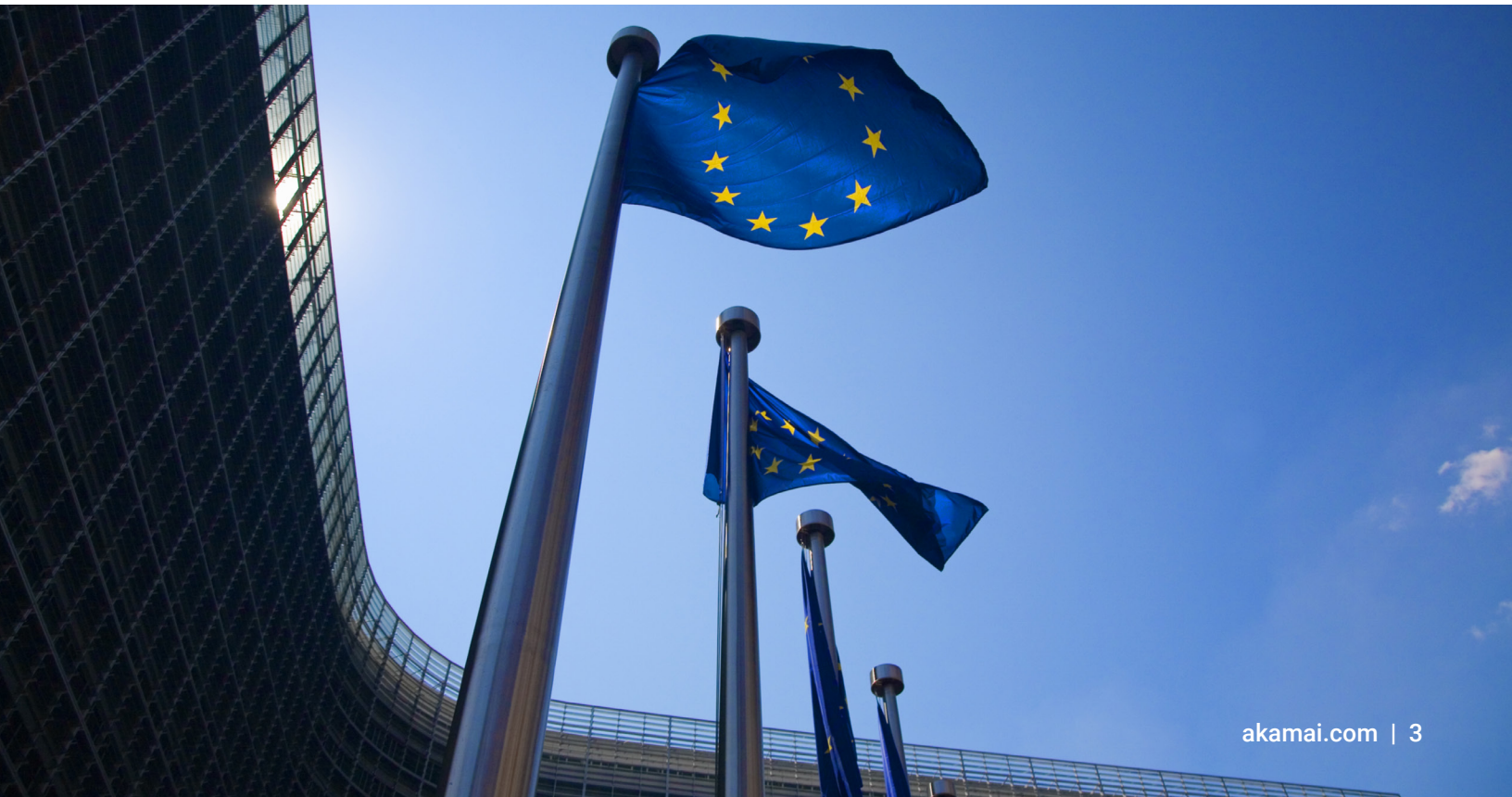
Einführung zur DORA-Verordnung

Die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, kurz „DORA“) zielt darauf ab, die Betriebszuverlässigkeit digitaler Systeme des Finanzdienstleistungssektors zu verbessern. Sie legt einen umfassenden Rahmen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT) fest und gilt für eine Vielzahl von Finanzunternehmen und IKT-Drittdienstleistern. In der DORA-Verordnung, die am 17. Januar 2025 in Kraft tritt, werden strenge Anforderungen in Bezug auf fünf wesentliche Säulen festgelegt:

Risiko-management | **Meldung von Vorfällen** | **Tests der digitalen operationalen Resilienz** | **Management des IKT-Drittparteien-risikos** | **Austausch von Informationen und Erkenntnissen**

Die DORA-Verordnung wird höhere regulatorische Anforderungen mit sich bringen, die Finanzunternehmen dazu verpflichten, strengere Standards einzuhalten, um gegenüber Cyberangriffen, Systemausfällen und sonstigen digitalen Risiken ihre operationale Resilienz zu gewährleisten. Dazu gehören regelmäßige Audits, Complianceprüfungen und eine strengere Berichterstattung an Aufsichtsbehörden. Ein erweitertes Risikomanagement wird zu einer Notwendigkeit werden, da die DORA-Verordnung einen umfassenden, integrierten Ansatz zur Ermittlung und Bewertung der mit kritischen Unternehmensdienstleistungen und digitalen Systemen verbundenen Risiken vorschreibt. Dazu müssen Finanzunternehmen zuverlässige Kontrollen implementieren und diese Risiken kontinuierlich überwachen und mindern. Viele von ihnen werden höhere Investitionen in Technologien tätigen müssen, um die DORA-Verordnung einhalten zu können.

Finanzunternehmen werden in fortschrittliche Technologien wie KI und ML investieren müssen, um durch bessere Bedrohungserkennung, automatisierte Abwehrmaßnahmen und prädiktive Analysen ihre operationale Resilienz und Reaktionsfähigkeit zu verbessern und zu beschleunigen. Es wird ebenfalls von entscheidender Bedeutung sein, das Augenmerk verstärkt auf das Management des Drittparteienrisikos zu legen. Denn Finanzunternehmen müssen sicherstellen, dass ihre Drittdienstleister zuverlässige Maßnahmen für operationale Resilienz eingerichtet haben. Dazu gehören die gebotene Sorgfaltspflicht ebenso wie regelmäßige Bewertungen und die Festsetzung eindeutiger vertraglicher Verpflichtungen zum Schutz vor digitalen Risiken. Die DORA-Verordnung verlangt auch mehr Transparenz: Finanzunternehmen werden ihre Maßnahmen für operationale Resilienz transparenter offenlegen müssen, um zu beweisen, dass sie effektiv auf digitale Störfaktoren reagieren können. Dazu müssen sie umfassende Aufzeichnungen führen und offen mit Regulierungsbehörden, ihrer Kundschaft und allen Beteiligten kommunizieren.



Relevanz der DORA-Verordnung für Finanzunternehmen

Die DORA-Verordnung wird in einer für Finanzunternehmen kritischen Zeit eingeführt, um der zunehmenden Häufigkeit und Komplexität von Cyberbedrohungen zu begegnen. In den letzten zwei Jahrzehnten war der Finanzdienstleistungssektor laut Internationalem Währungsfonds eines der attraktivsten Ziele für Cyberkriminelle. Das Ausmaß der Verluste hat sich seit 2017 auf 2,5 Milliarden US-Dollar mehr als vervierfacht, und indirekte Verluste, etwa durch Rufschäden oder verstärkte Sicherheitsmaßnahmen, sind deutlich höher. Angriffe kompromittieren nicht nur sensible Finanzinformationen, sondern bringen auch erhebliche Risiken für die allgemeine Stabilität und Integrität der Finanzsysteme mit sich. Finanzunternehmen setzen zunehmend auf digitale Infrastrukturen. Das macht sie aufgrund der Komplexität und Interkonnektivität ihrer Systeme anfälliger für Cyberbedrohungen. Diese Schwachstellen nutzen Angreifende aus. Dabei kommen oft fortschrittliche Methoden wie laterale Netzwerkbewegungen zum Einsatz, um sich Zugriff auf wertvolle Daten zu verschaffen oder Störungen zu verursachen. So wechseln Cyberkriminelle von einem System zum anderen, was die Erkennung und Vorbeugung schädlicher Aktivitäten erschwert und so das Risiko erheblicher Sicherheitsverletzungen oder Betriebsstörungen steigert.

Die Einführung der DORA-Verordnung ist eine proaktive Abwehrmaßnahme gegen diese dynamischen Bedrohungen. Durch die Schaffung eines harmonisierten Rahmens für digitale Resilienz in den EU-Mitgliedsstaaten soll sie ein gleichbleibendes Maß an Sicherheit und operationaler Resilienz im gesamten Finanzsektor gewährleisten. Diese Einheitlichkeit ist entscheidend, da sie das Vertrauen in die digitale Infrastruktur der Branche stärkt und Finanzunternehmen dabei in die Lage versetzt, technologischen Störungen standzuhalten (und sich davon zu erholen). Die vorausschauende Aufsetzung der DORA-Verordnung spiegelt einen strategischen Wandel wider: Statt auf Vorfälle bloß zu reagieren, sollen potenzielle Risiken vor deren Auftreten vorhergesehen und gemindert werden. Dieser Ansatz dient nicht nur dem Schutz einzelner Unternehmen, sondern des Finanzwesens im weiteren Sinne vor systemischen Risiken. Der Schwerpunkt der Verordnung liegt darauf, die Reaktionsmaßnahmen bei Vorfällen und das Management des Drittparteienrisikos zu verbessern. Dies unterstreicht, wie wichtig es ist, bei der Cybersicherheit einen umfassenden und integrierten Ansatz zu verfolgen.

Ein weiterer wesentlicher Aspekt der DORA-Verordnung ist die Transparenz: Finanzunternehmen müssen einen besseren Einblick in ihre Maßnahmen für operationale Resilienz gewähren und so beweisen, dass sie in der Lage sind, effektiv auf digitale Störungen zu reagieren. Diese Transparenz ist entscheidend, um das Vertrauen der Regulierungsbehörden, der Kundschaft und aller Beteiligten aufrechtzuerhalten, und sie unterstreicht das Engagement des Finanzinstituts für den Schutz seiner digitalen Infrastruktur. Die Relevanz der DORA-Verordnung geht über den Compliance-Aspekt hinaus. Sie steht für einen grundlegenden Wandel in der Herangehensweise von Finanzunternehmen an Cybersicherheit und operationale Resilienz: Indem sie die DORA-Anforderungen einhalten, schützen sie sich nicht nur vor aktuellen und zukünftigen Bedrohungen, sondern positionieren sich auch als vertrauenswürdige Institutionen in einer zunehmend digitalen Finanzwelt.

Akamai unterstützt Finanzunternehmen bei der Einhaltung der DORA-Anforderungen

Wir nutzen die Größe und umfassenden Bedrohungsanalysen unserer globalen Plattform, um Finanzunternehmen bei der Prävention, Erkennung und Minderung von Cyberbedrohungen sowohl in lokalen als auch in Cloud-Umgebungen zu helfen, damit sie die Komplexität der veränderlichen Compliance-Anforderungen bewältigen können. Unsere Lösungen leisten bei den wesentlichen Säulen der DORA-Verordnung Unterstützung: im Risikomanagement, bei der Meldung von Vorfällen, bei Tests der digitalen operationalen Resilienz, im Management des IKT-Drittparteienrisikos sowie beim Austausch von Informationen und Erkenntnissen. Das Ergebnis: umfassende, zuverlässige Cybersicherheit.

API Security

Akamai API Security bietet umfassende API-Erkennung, kontrolliert die Sicherheitslage und verfügt über KI-/ML-basierten Laufzeitschutz. Diese Funktionen sind unerlässlich, um fortschrittliche API-Angriffe in Echtzeit zu erkennen und abzuwehren. Proaktive Sicherheitstests und Echtzeitanalysen ermöglichen Finanzunternehmen, umgehend das API-Verhalten zu prüfen, auf Bedrohungen zu reagieren und sensible Daten zu schützen. Dies hilft ihnen, die Anforderungen der DORA-Verordnung in Bezug auf das IKT-Risikomanagement und die Meldung von Vorfällen einzuhalten.

Die Minderung der Risiken im Zusammenhang mit Shadow-APIs, anfälligen APIs und API-Missbrauch stellt aufgrund mangelnder Transparenz und Überwachung eine erhebliche Herausforderung dar. Zur effektiven API-Sicherheit gehören eine umfassende Erkennung und Katalogisierung, Bedrohungserkennung in Echtzeit und KI-gesteuerte Schutzmechanismen, um eine kontinuierliche Überwachung und Abwehr API-bezogener Bedrohungen zu gewährleisten und die vorgeschriebenen Standards der DORA-Verordnung einzuhalten.

Akamai Guardicore Segmentation

Akamai Guardicore Segmentation ermöglicht Finanzunternehmen, ihre Netzwerke in sichere Segmente zu unterteilen. Dadurch wird das Risiko lateraler Bewegungen durch Cyberbedrohungen erheblich verringert. Diese Technologie verbessert das IKT-Risikomanagement und die Tests der digitalen operationalen Resilienz und entspricht somit den Zielen der DORA-Verordnung. Kompromittierte Assets werden isoliert und Angreifende in ihren lateralen Netzwerkbewegungen eingeschränkt. So trägt die Mikrosegmentierung dazu bei, eine zuverlässige Sicherheitslage aufrechtzuerhalten und effektive Reaktionsmaßnahmen bei Vorfällen zu erleichtern.

Akamai Guardicore Segmentation bietet umfassende Einblicke in Anwendungsabhängigkeiten und eine präzise Durchsetzung der Richtlinien, sodass eine kontinuierliche Verwaltung der Mikrosegmentierungsrichtlinien gewährleistet wird. Die Plattform unterstützt sowohl agentbasierte als auch agentlose Bereitstellungsoptionen – mit flexiblen Einsatzmöglichkeiten für verschiedene Umgebungen, einschließlich PaaS-, IoT- und OT-Umgebungen in der Cloud. Mithilfe KI-gestützter Richtlinienerstellung und intuitiver Workflows vereinfacht Akamai Guardicore Segmentation den Prozess der Mikrosegmentierung. Somit können Finanzunternehmen Sicherheitsrichtlinien schnell implementieren und an veränderte Netzwerkbedingungen anpassen. Dieser umfassende Ansatz reduziert nicht nur die Angriffsfläche, sondern unterstützt auch bei der Einhaltung gesetzlicher Anforderungen an die digitale operationale Resilienz.

Edge DNS

Akamai Edge DNS sorgt für hohe Verfügbarkeit und Performance von DNS-Diensten und schützt dabei die lokale, cloudbasierte und hybride DNS-Infrastruktur. Diese Lösung ist zur Aufrechterhaltung der Servicekontinuität und für den Schutz vor groß angelegten Cyberbedrohungen unerlässlich und erfüllt die Anforderungen der DORA-Verordnung an das IKT-Risikomanagement und die Meldung von Vorfällen.

App & API Protector

Akamai App & API Protector bekämpft Layer-7-Angriffe mit umfassenden Schutzmaßnahmen, einschließlich der Abwehr von DDoS-Angriffen (Distributed Denial of Service), Bots und Exploits in den OWASP Top 10. Diese Lösung schafft zuverlässige Sicherheit für Webanwendungen und APIs, was für die Einhaltung der DORA-Verordnung in Bezug auf das IKT-Risikomanagement und die Meldung von Vorfällen entscheidend ist.

Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance unterstützt bei der PCI-Compliance und schützt Websites vor JavaScript-Angriffen. Dadurch können Finanzunternehmen sensible Daten ihrer Kundschaft schützen und die strengen Anforderungen der DORA-Verordnung und anderer Vorschriften einhalten.

Prolexic

Akamai Prolexic schützt die Infrastruktur vor DDoS-Angriffen. Die Lösung bietet zuverlässige Abwehrmechanismen, um selbst bei groß angelegten Angriffen Verfügbarkeit und Zuverlässigkeit zu gewährleisten. Dies entspricht den Zielen der DORA-Verordnung, die digitale operationale Resilienz und die Reaktionsmaßnahmen bei Vorfällen zu verbessern.

Bot Manager

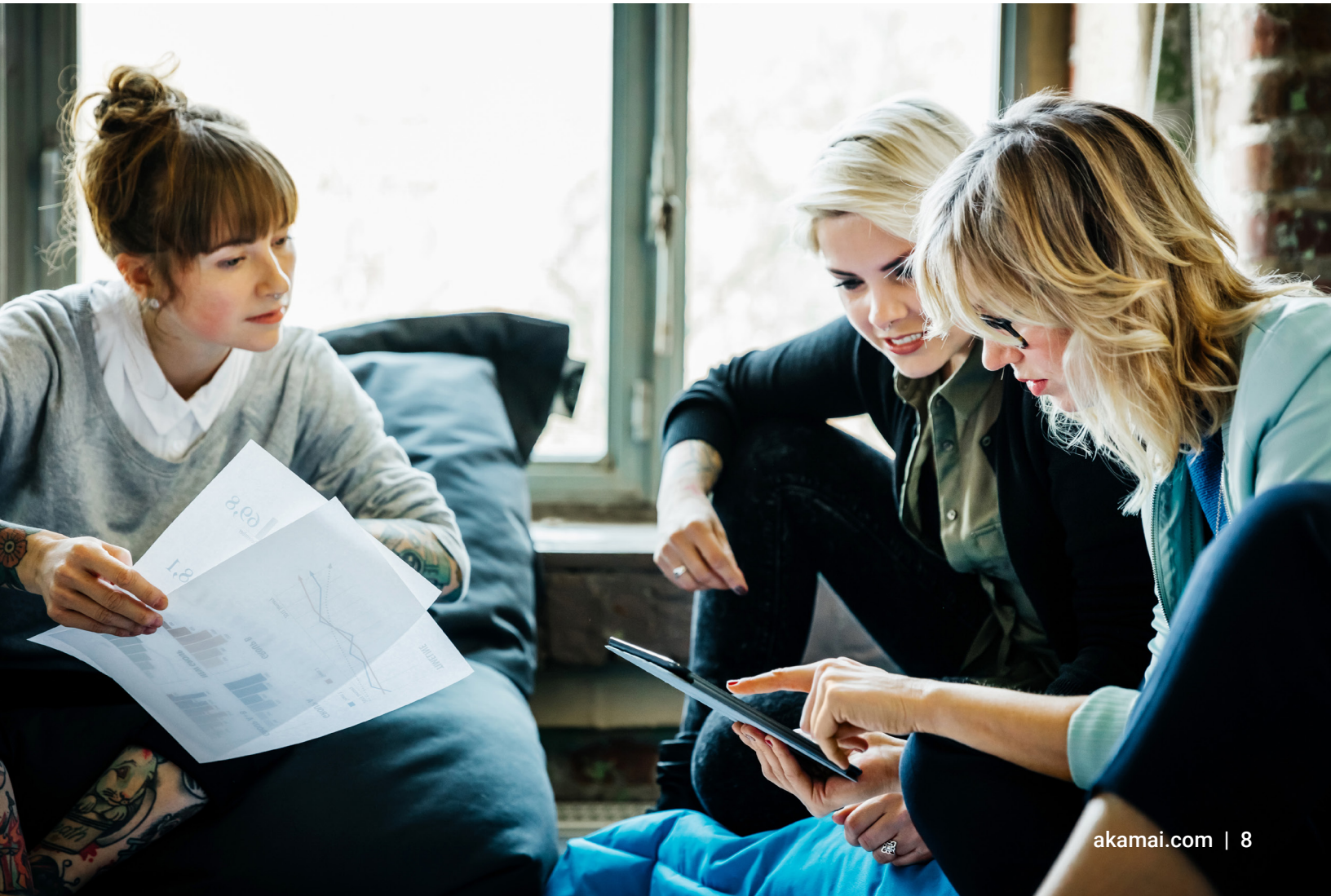
Akamai Bot Manager bietet fortschrittliches Bot-Management, das raffinierte bösartige Bots erkennt und beseitigt, aber gute Bots zulässt. Dies unterstützt legitimen Traffic, um für ein nahtloses Anwendungserlebnis zu sorgen und Unternehmen zu helfen, die Anforderungen der DORA-Verordnung an das IKT-Risikomanagement einzuhalten.

Account Protector

Akamai Account Protector erkennt und verhindert die Übernahme von Konten, die missbräuchliche Erstellung von Konten und Credential Stuffing. Diese Funktion ist entscheidend, um die Konten Ihrer Kundschaft zu schützen und ihr Vertrauen aufrechtzuerhalten. Sie steht somit im Einklang mit der DORA-Verordnung, die einen Fokus auf Zuverlässigkeit im IKT-Risikomanagement und bei der Meldung von Vorfällen legt.

Content Protector

Akamai Content Protector verhindert, dass Scraper Inhalte stehlen und die Konversionsraten senken. Diese Lösung sichert proprietäre Inhalte und unterstützt die Ziele der DORA-Verordnung, digitale Assets zu schützen und die operationale Resilienz zu verbessern.



Detaillierte Anforderungen und Akamai-Lösungen

Governance und Organisation

Governance der Sicherheit: Das Security Operations Command Center von Akamai bietet rund um die Uhr Überwachungs- und Reaktionsdienste, um die sicherheitsbezogene Governance kontinuierlich zu beobachten.

Integration von Security Information and Event Management (SIEM): Die Akamai-Lösung zur SIEM-Integration bietet eine Möglichkeit, SIEM-Ereignisse in Analysetools wie Splunk, QRadar und ArcSight bereitzustellen, sodass Sie Akamai-Sicherheitsereignisse in Ihre gesamte Ereignis- und Sicherheitsinfrastruktur integrieren können.

Governance, Risk & Compliance (GRC): Das Akamai Control Center bietet eine zentrale Oberfläche zur Verwaltung der Produkte und Services von Akamai. Es bietet Unternehmen den Zugriff, die Einblicke und die Kontrolle, die sie benötigen, um Risikomanagement-, Compliance- und regulatorische Anforderungen zu erfüllen, und gleichzeitig optimale Onlineerlebnisse.

IKT-Risikomanagementrahmen

Software für Risikomanagement: Akamai Secure Internet Access bietet erweiterten Schutz vor Bedrohungen einschließlich Malware und Phishing.

Endpoint Protection Platforms: Akamai Bot Manager unterstützt Sie bei Management und Abwehr bösartigen Bot-Traffics.

Tools für Sicherheitsmanagement: Die Lösungen von Akamai bieten kontinuierliche Scans und Schwachstellenbewertungen von IKT-Systemen.

Behandlung IKT-bezogener Vorfälle

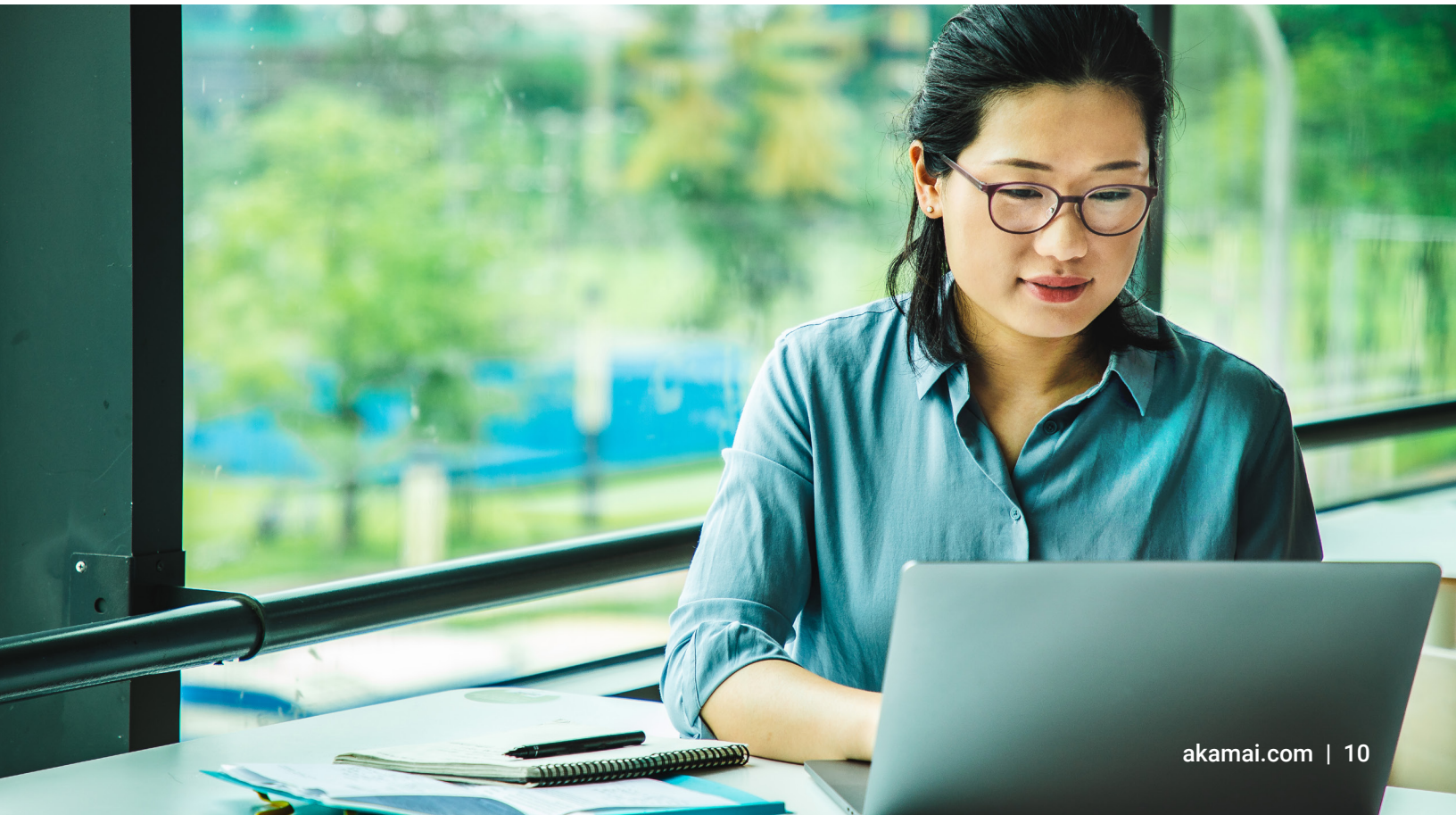
Plattformen für Vorfallsreaktion: Die Akamai-Services für Vorfallsreaktion automatisieren und koordinieren die Reaktionsmaßnahmen bei Vorfällen.

Systeme zur Verfolgung von Vorfällen: Die Lösungen von Akamai verfolgen und verwalten die Meldung und Behebung von Vorfällen.

Tests der digitalen operationalen Resilienz

Services für Penetrationstests: Akamai bietet im Rahmen des Kundenservice Penetrationstests und andere Sicherheitsbewertungen an.

Red-Team-/Blue-Team-Übungen: Akamai führt regelmäßige Sicherheitsübungen durch, um die Reaktion des Unternehmens zu bewerten und zu verbessern und die Einhaltung gesetzlicher Vorschriften sicherzustellen.



Management des Drittparteienrisikos

Plattformen für Drittparteienrisiko-Management: Mit den Akamai-Sicherheitsprodukten, einschließlich Web Application Firewall (WAF) und API Gateway, lassen sich Risiken managen und mindern.

Software für Vertragsmanagement: Die Lösungen von Akamai unterstützen bei der Verwaltung und Einhaltung vertraglicher Verpflichtungen.

Plattformen für Bedrohungsanalysen: Die Threat Intelligence Services von Akamai liefern aktuelle Informationen zu aufkommenden Bedrohungen mithilfe externer und interner Feeds.

Financial Services Information Sharing and Analysis Center (FS-ISAC): Akamai ist Gründungsmitglied des „Critical Providers Program" des FS-ISAC. Durch interne Zusammenarbeit und den Austausch von Bedrohungsinformationen lassen sich Schwachstellen, Ausfälle, Risiken und Verstöße schnell kommunizieren. Daher sind diese Prozesse weiterhin entscheidend, um die Infrastruktur der Finanzdienstleistungsbranche erfolgreich zu sichern. Unser einzigartiger Zugriff auf Traffic und Angriffsdaten ermöglicht uns, gemeinsam mit den Mitgliedern an Studien zu arbeiten und Best Practices auszutauschen.

Überwachung und Durchsetzung

Audit- und Compliancetools: Die Compliancelösungen von Akamai helfen bei der Prüfung und Einhaltung gesetzlicher Anforderungen.

Monitoring- und Reportinglösungen: Das Control Center bietet umfassende Funktionen für das Monitoring und Reporting.

Kundenreferenzen als Nachweis der Effektivität von Akamai

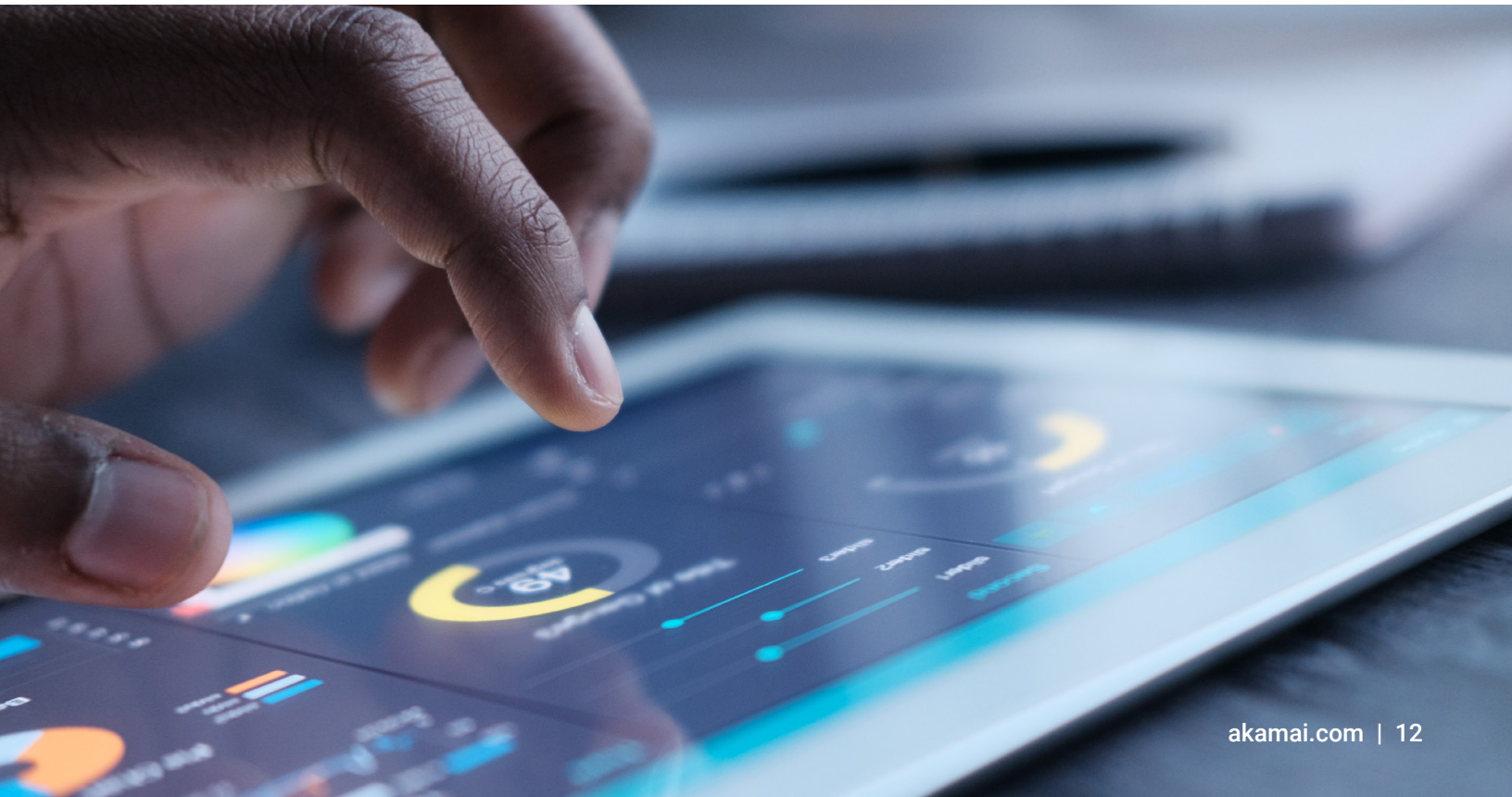
Um festzustellen, inwiefern sich Akamai dafür eignet, bei der Einhaltung gesetzlicher Vorschriften zu helfen, kann ein genauer Blick auf die Erlebnisse der Kundschaft aufschlussreich sein. Hier einige relevante Beispiele:

Großes Versicherungsunternehmen: Diese Kundenreferenz zeigt, wie das Versicherungsunternehmen die Lösungen von Akamai nutzt, um die Sicherheit und Performance zu verbessern. Die Angebote von Akamai helfen bei der Abwehr von DDoS-Angriffen und der Sicherung von APIs, die zur Aufrechterhaltung des IKT-Risikomanagements und der Reaktionsmaßnahmen bei Vorfällen gemäß DORA-Verordnung entscheidend sind.

Cashflows: Cashflows nutzt die Sicherheitslösungen von Akamai, um seine in der Cloud gehostete Zahlungsplattform zu schützen. Diese Kundenreferenz zeigt, wie Akamai die Einhaltung von Sicherheitsstandards gewährleistet und vor Bedrohungen wie DDoS-Angriffen schützt, um die kontinuierliche Verfügbarkeit und Sicherheit von Zahlungsdiensten sicherzustellen. Dies entspricht den Anforderungen der DORA-Verordnung an das IKT-Risikomanagement und die Tests der digitalen operationalen Resilienz.

LANDBANK: Als größte staatliche Bank auf den Philippinen verlässt sich die LANDBANK auf Akamai, um ihre Onlineanwendungen zu sichern, sich vor Cyberbedrohungen zu schützen und die Digitalisierung zu vereinfachen. Diese Kundenreferenz ist besonders wichtig, um zu verstehen, wie die Lösungen von Akamai dazu beitragen können, Drittparteienrisiken zu managen und zuverlässige Prozesse des Vorfallsmanagements sicherzustellen.

Diese Beispiele veranschaulichen, dass die umfassenden Akamai-Sicherheitslösungen und Funktionen für proaktives Bedrohungsmanagement Finanzunternehmen dabei unterstützen können, die DORA-Anforderungen zu erfüllen – einschließlich IKT-Risikomanagement, Meldung von Vorfällen, Tests der digitalen operationalen Resilienz und Management des Drittparteienrisikos.



Fazit

Die DORA-Verordnung stellt einen erheblichen Wandel in der Gesetzeslage für Finanzunternehmen dar und verlangt umfassende und proaktive Maßnahmen zur Cybersicherheit. Die Lösungssuite von Akamai bietet einen zuverlässigen Rahmen zur Unterstützung von Finanzunternehmen (1) bei der Erfüllung der strengen Anforderungen der DORA-Verordnung und (2) bei der Gewährleistung einer besseren digitalen operationalen Resilienz, eines zuverlässigen IKT-Risikomanagements und einer effektiven Reaktionsfähigkeit bei Vorfällen. Unter Einsatz der fortschrittlichen Technologien von Akamai können Finanzunternehmen die komplexen Compliance-Anforderungen der DORA-Verordnung zuversichtlich bewältigen und ihre Betriebsabläufe vor der veränderlichen Bedrohungslage schützen.

Weitere Informationen 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.