AKAMAI-LÖSUNGSÜBERBLICK

Digital Operational Resilience Act

Akamai bereitet Finanzunternehmen auf DORA-Compliance vor

Der Digital Operational Resilience Act (DORA) ist ein neuer wichtiger Rechtsakt in Europa, der ein strengeres Regelwerk für regulierte Finanzunternehmen festlegt, indem ein verbesserter Rahmen für die digitale operationale Resilienz vorgeschrieben wird, der nicht nur Finanzunternehmen, sondern auch deren Drittanbieter für Informations- und Kommunikationstechnologie (IKT) umfasst. DORA tritt am 17. Januar 2025 in Kraft.

Geltungsbereich von DORA

DORA gilt für Finanzunternehmen weltweit, die auf EU-Märkten tätig sind. Der Geltungsbereich umfasst sowohl traditionelle Unternehmen wie Banken, Wertpapierfirmen und Kreditinstitute als auch nichttraditionelle Unternehmen wie Serviceanbieter für Krypto-Assets und Crowdfunding-Plattformen.

Darüber hinaus sieht DORA auch für Unternehmen, die keine Finanzunternehmen sind und im Allgemeinen von Finanzvorschriften ausgenommen sind, bestimmte Verpflichtungen vor. Beispielsweise müssen Drittanbieter, die Finanzunternehmen IKT-Systeme und -Dienste bereitstellen – etwa Cloud-Service-Provider und Rechenzentren – ebenfalls bestimmte DORA-Anforderungen erfüllen. Außerdem umfasst DORA auch Unternehmen, die wichtige Informationsservices bereitstellen, wie Kreditwürdigkeitsservices und Anbieter von Datenanalysen. IKT-Drittanbieter, die von den Europäischen Aufsichtsbehörden (ESAs) als kritisch eingestuft werden, stehen unter der direkten Aufsicht eines durch die ESAs benannten federführenden Koordinators.

Akamai unterstützt die Ziele der Finanzbehörden und bietet sowohl als wichtige Drittpartei als auch als Anbieter seine Hilfe an, damit unsere Kunden die erwarteten Rahmenregelungen erfüllen können. Wir werden Anfragen bearbeiten und unseren Kunden ein besseres Verständnis über die Möglichkeiten der operationalen Resilienz mit Akamai ermöglichen.

Die fünf Säulen von DORA

Der umfassende Ansatz von DORA basiert auf fünf zentralen Säulen, die jeweils auf unterschiedliche Facetten der digitalen operationalen Resilienz zugeschnitten sind.

Risiko-management | Meldung von Vorfällen | Tests der digitalen operationalen Resilienz | IKT-Drittparteien-risiko | Austausch von Informationen und Erkenntnissen

Risikomanagement

- Mit dem Akamai Control Center (ACC) und seinen integrierten Sicherheitsanalysedashboards, SLA-Überwachung und Einblicken in die Dokumentation (inkl. Richtlinien und Berichten) erhalten Sie umfassende Transparenz in ihre Service-Performance.
- Jährlich durchgeführte Bewertungen des Drittparteienrisikomanagements von Akamai bieten Einblicke in die Unternehmenssicherheit und die mit dem Service verbundenen Risiken.
- Mit den Zero-Trust- und Segmentierungsprodukten von Akamai können Kunden ihre Risiken im Zusammenhang mit Ransomware und der Erhöhung interner Zugriffsrechte reduzieren und beheben.
- Kontinuierliche Audits der Sicherheit von Akamai anhand branchenspezifischer und regionaler Sicherheitsframeworks wie SOC 2, ISO 27001 oder dem deutschen BSI ermöglichen eine bessere Bewertung des Risikostatus des Unternehmens.

Meldung von Vorfällen

- Rund um die Uhr verfügbare Abdeckung mit Benachrichtigungssystem für alle kundenrelevanten Vorfälle innerhalb der erwarteten Fristen.
- Globale Abdeckung wird mit auf Abruf verfügbarer Kundenservice- und Sicherheitsspezialisten in mehreren Betriebszentren in allen wichtigen Regionen gewährleistet.
- Vorfallsinformationen werden über akamaistatus.com, den Community Service und das ACC bereitgestellt.

Akamai

Tests der digitalen operationalen Resilienz

- Hochmodernes Resilienzmodell, das getestet wurde, um den größten DDoS-Angriffen der IKT-Branche standzuhalten.
- Vierteljährliche Tests der Infrastruktur und halbjährliche Tests der Personalbereitschaft zur Notfallwiederherstellung.
- Fortlaufende Erfahrungen und Verbesserungen werden jedes Jahr umgesetzt, um kontinuierliche interne und compliancebasierte Penetrationstests zu gewährleisten, die dem TIBER-EU-Framwork für bedrohungsorientierte Drittpartei-Penetrationstests zur Bewertung des bestehenden Resilienzmodells entsprechen.

IKT-Drittparteienrisiko

- Akamai bewertet alle Anbieter und Drittparteien, bevor wir diese onboarden und ihre Services und Plattformen nutzen. Jeder Anbieter und jedes Produkt wird speziellen Prüfungen unterzogen, die sich auf seine Servicesicherheit, die Art und Weise der Informationsverarbeitung, die Einhaltung von Datenschutzgesetzen und die Frage beziehen, ob der finanzielle Status des Unternehmens Risiken für Akamai birgt.
- Ein spezielles TPRM-Team (Third-Party Risk Management) stellt sicher, dass Anbieter vertraglich die Regeln für die Zusammenarbeit mit Akamai einhalten. Jeder wichtige Anbieter muss sich einer jährlichen Überprüfung der Einhaltung vertraglicher Verpflichtungen unterziehen – und im Falle einer Nichteinhaltung bestehen Ausstiegspläne.

Austausch von Informationen und Erkenntnissen

- Die Akamai Security Intelligence Group führt kontinuierliche Untersuchungen zu neuen Bedrohungen durch, die IKT-Anbieter und Kunden von Akamai betreffen. Wir verwenden ein ausgeklügeltes Netzwerk aus Honeypots und Informationen, die außerhalb der global verteilten Edge von Akamai gesammelt wurden, um Indicators of Compromise (IOCs) zu identifizieren und sie über verschiedene Kommunikationskanäle weiterzugeben.
- Akamai beteiligt sich an der Community zum Austausch von Cybersicherheitsinformationen der FS-ISAC und stellt dort Informationsauszüge der Kategorien TLP Green und TLP Amber sowie Fallstudien zur Verfügung.

„Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Teil ihres gesamten Risikomanagementsystems. So können sie IKT-Risiken schnell, effizient und umfassend angehen und ein hohes Maß an digitaler operationaler Resilienz gewährleisten.“ (Artikel 6)

Das Framework für die operationale Resilienz erfordert kontinuierliche Aufmerksamkeit, um die IKT- und Informationsassets des Unternehmens zu schützen. Dies umfasst den kontinuierlichen Schutz von Software, physischer Geräte und Daten. Das Framework erfordert außerdem regelmäßige Aktualisierungen (mindestens einmal jährlich), die durch größere IKT-Vorfälle, Aufsichtsrichtlinien oder Erkenntnisse aus Test- oder Auditprozessen ausgelöst werden.

Was Akamai-Lösungen bewirken

Akamai orientiert sich an den Zielen der Behörden für ein robustes europäisches Finanzsystem und schätzt den kontinuierlichen Dialog. Wir halten uns gewissenhaft an Vorschriften und unterstützen unsere Kunden dabei, unseren Ansatz für kritische Drittanbieter zu verstehen und gleichzeitig ihre operationale Resilienz zu verbessern.

Mit Akamai können Finanzinstitute Compliance-Herausforderungen, einschließlich Unklarheiten und Unsicherheiten bezüglich behördlicher Vorschriften – ob DORA oder zukünftige Auflagen – mithilfe umfassender Sicherheitsmaßnahmen, die alles von Anwendungsworkloads und APIs bis hin zur Anwendungsinfrastruktur umfassen, effektiv bewältigen. Die Sicherheit wird zu einem wichtigen Bestandteil des Compliance-Toolkits, das nachhaltige, effektive Veränderungen ermöglicht und vor allem Stärkung des Kundenvertrauens in Finanzinstitute und den Finanzmarkt im weiteren Sinne fördert.

Erfahren Sie mehr über DORA.