PRÉSENTATION AKAMAI

Règlement sur la résilience opérationnelle digitale du secteur financier

Akamai aide les entités financières à se mettre en conformité avec le règlement DORA

Le règlement sur la résilience opérationnelle numérique (DORA) est un nouveau texte législatif européen majeur qui établit des règles plus strictes pour les entités financières réglementées en exigeant un cadre amélioré de résilience opérationnelle digitale couvrant non seulement les entités financières, mais aussi leurs fournisseurs tiers de technologies de l'information et de la communication (TIC). Le règlement DORA entrera en vigueur le 17 janvier 2025.

Champ d'application du règlement DORA

Le règlement DORA s'applique aux entités financières du monde entier qui opèrent sur les marchés de l'UE. Le champ d'application comprend les entités traditionnelles telles que les banques, les entreprises d'investissement et les établissements de crédit, ainsi que les entités non traditionnelles telles que les fournisseurs de services d'actifs cryptographiques et les plateformes de crowdfunding.

En outre, le règlement DORA impose certaines obligations aux entités qui ne sont pas des entités financières et qui sont généralement exemptées des réglementations financières. Par exemple, les fournisseurs de services tiers qui proposent aux entreprises financières des systèmes et des services TIC, comme les fournisseurs de services cloud et les centres de données, doivent se conformer à certaines exigences du règlement DORA. En outre, le règlement DORA inclut les entreprises qui fournissent des services d'information essentiels à des tiers, comme les services de notation de crédit et les fournisseurs de services d'analyse de données. Les fournisseurs tiers de TIC désignés comme essentiels par les Autorités européennes de surveillance (AES) feront l'objet d'une évaluation par un superviseur principal nommé par les AES.

Akamai contribuera à la réalisation des objectifs des autorités financières et fournira une assistance à la fois en tant que tiers critique et en tant que fournisseur, en aidant nos clients à se conformer aux régimes cadres attendus. Nous coopérerons pour répondre aux demandes de renseignements et aider à comprendre les moyens par lesquels nous assurons la résilience opérationnelle.

Les 5 piliers du règlement DORA

L'approche globale du règlement DORA s'appuie sur cinq piliers fondamentaux, chacun d'entre eux étant conçu pour traiter des aspects distincts de la résilience opérationnelle digitale.

Gestion des risques | Signalement des incidents | Tests de résilience opérationnelle digitale | Risques liés aux TIC pour les tiers | Partage d'informations et de renseignements

Gestion des risques

- Visibilité complète sur les performances du service grâce à l'Akamai Control Center (ACC) et à ses tableaux de bord analytiques de sécurité intégrés, à la surveillance de l'accord de niveau de service (SLA) et à l'aperçu de la documentation, y compris les politiques et les rapports.
- Des évaluations contractuelles de la gestion des risques par des tiers, effectuées chaque année sur Akamai, permettent de mieux comprendre la sécurité de l'entreprise et d'évaluer les risques associés au service.
- Les produits Zero Trust et de segmentation d'Akamai aident les clients à minimiser et à réduire les risques liés à une attaque par ransomware et aux menaces d'élévation de l'accès interne.
- L'audit continu de la sécurité d'Akamai à l'aide de cadres de sécurité sectoriels et régionaux, tels que SOC 2, ISO 27001 ou le BSI allemand, permet de mieux évaluer l'état des risques de l'entreprise.

Signalement des incidents

- Couverture 24 h/24 et 7 j/7 avec un système de notification pour tous les incidents ayant un impact sur les clients dans les délais prévus.
- Couverture mondiale, avec des spécialistes du service client et de la sécurité en attente dans plusieurs centres d'opérations dans toutes les grandes zones géographiques.
- Fourniture d'informations sur les incidents via akamaistatus.com, le service communautaire et l'ACC.

Akamai

Tests de résilience opérationnelle digitale

- Un modèle de résilience de pointe a été testé pour résister aux plus grandes attaques DDoS que le secteur des TIC ait connues.
- Tests trimestriels de l'infrastructure et tests semestriels de l'état de préparation du personnel pour la reprise en cas de sinistre.
- Enseignements continus et améliorations mises en œuvre au fil des ans pour garantir un processus continu de tests de pénétration internes et fondés sur la conformité, alignés sur les tests de pénétration TIBER-UE menés par des tiers et évaluant le modèle de résilience existant.

Risques liés aux TIC pour les tiers

- Akamai évalue tous ses fournisseurs et tiers avant de les intégrer et d'utiliser leurs services et plateformes. Chaque fournisseur et chaque produit font l'objet de vérifications spécifiques concernant la sécurité de leurs services, la manière dont ils traitent les informations, la conformité à la législation sur la protection de la vie privée et la question de savoir si la situation financière de l'entreprise présente des risques pour Akamai.
- Une équipe dédiée à la gestion des risques par des tiers veille à ce que les fournisseurs respectent contractuellement les règles d'engagement d'Akamai. Chaque fournisseur essentiel fait l'objet d'un contrôle annuel de conformité aux obligations contractuelles, et des plans de sortie sont mis en place en cas de non-conformité.

Partage d'informations et de renseignements

- Le groupe Security Intelligence d'Akamai mène des recherches continues sur les menaces émergentes visant les fournisseurs de TIC et les clients d'Akamai. Un réseau sophistiqué de pots de miel et de renseignements recueillis hors de la bordure de l'Internet distribuée mondialement d'Akamai est utilisé pour identifier les indicateurs d'infection, qui sont ensuite partagés sur différents canaux de communication.
- Akamai participe à la communauté de partage de renseignements de FS-ISAC, en fournissant des échantillons de renseignements TLP verts et orange et des études de cas.

« Les entités financières doivent adopter, dans le cadre de leur système global de gestion des risques, un cadre de gestion des risques liés aux TIC qui soit solide, complet et bien documenté et qui leur permette de traiter les risques liés aux TIC de manière rapide, efficace et globale et de garantir un niveau élevé de résilience opérationnelle digitale. » (Article 6)

Le cadre de résilience opérationnelle nécessite une attention permanente pour protéger les TIC et les actifs d'information de l'organisation. Il s'agit notamment de protéger en permanence les logiciels, les équipements physiques et les données. Le cadre prévoit des mises à jour régulières, au moins une fois par an, en cas d'incidents majeurs liés aux TIC, de directives de surveillance ou d'observations issues des processus de test ou d'audit.

Comment Akamai vous aide

Akamai est en phase avec les objectifs des autorités concernant la solidité du système financier européen et apprécie les échanges continus. Nous respectons scrupuleusement les réglementations et nous aiderons nos clients à comprendre notre approche de tiers essentiel tout en améliorant leur résilience opérationnelle.

Grâce à Akamai, les institutions financières peuvent gérer efficacement les défis de conformité, notamment l'ambiguïté et l'incertitude réglementaires, qu'il s'agisse du règlement DORA ou de futurs mandats, grâce à des mesures de sécurité complètes couvrant les charges de travail et les API des applications jusqu'à l'infrastructure des applications. Dès lors, la sécurité devient un élément essentiel de la boîte à outils réglementaire, facilitant un changement durable et efficace et, surtout, renforçant la confiance des clients dans les institutions financières et le marché financier au sens large.

En savoir plus sur le règlement DORA.