LIVRE BLANC

Soutenir les objectifs du règlement DORA avec Akamai

Le concept de résilience opérationnelle numérique a considérablement évolué au fil des ans, en particulier au sein des services financiers. Dans un premier temps, les entités financières se sont concentrées sur la reprise après sinistre et la planification de la continuité des activités. Ces premiers efforts étaient essentiellement réactifs et visaient à rétablir les services après une interruption. Lorsque les cybermenaces sont devenues plus fréquentes et plus sophistiquées, l'accent a été mis sur des mesures plus proactives. Les entités financières ont commencé à mettre en œuvre des protocoles de cybersécurité robustes, des mises à jour régulières des systèmes et des programmes de formation des employés afin de prévenir les perturbations avant qu'elles ne se produisent. L'avènement de technologies avancées telles que les grands modèles de langage (LLM), l'intelligence artificielle (IA) et l'apprentissage automatique (ML) a révolutionné l'approche de la résilience opérationnelle. Cependant, ces mêmes technologies ont également révolutionné les vecteurs de menace, augmentant la complexité et la fréquence des menaces. Par conséquent, la résilience opérationnelle doit s'adapter en permanence à ces défis en constante évolution.

Ces technologies permettent l'analyse prédictive, la détection automatisée des menaces et des temps de réponse plus rapides, ce qui améliore considérablement les capacités de résilience. La réglementation de plus en plus stricte a également favorisé l'évolution de la résilience opérationnelle numérique. Des réglementations telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE) ont contribué à établir des normes plus élevées en matière de protection des données et de continuité opérationnelle. Toutefois, la complexité et la fréquence croissantes des cybermenaces sont les principaux facteurs qui obligent les entités financières à adopter des stratégies de résilience plus complètes. Les approches actuelles de la résilience opérationnelle numérique englobent désormais la gestion holistique des risques. Cela comprend non seulement des mesures de protection techniques, mais aussi des cadres de gouvernance, la gestion des risques liés aux tiers, des pratiques de surveillance et d'amélioration continues et le partage d'informations.

Présentation du règlement DORA

Le Règlement sur la résilience opérationnelle numérique (DORA) est un règlement de l'UE visant à renforcer la résilience opérationnelle numérique du secteur des services financiers. Il établit un cadre global pour la gestion des risques liés aux technologies de l'information et de la communication (TIC) et s'applique à un large éventail d'entités financières et de fournisseurs de services TIC tiers. Devant entrer en vigueur le 17 janvier 2025, le règlement DORA impose des exigences strictes dans cinq domaines clés :

Gestion des risques

Signalement des incidents

Test de résistance opérationnelle numérique

Gestion des risques liés aux TIC par des tiers

Partage d'informations et de renseignements

Le règlement DORA renforcera les exigences réglementaires, obligeant les entités financières à respecter des normes plus strictes pour garantir leur résilience opérationnelle face aux cyberattaques, aux pannes de système et aux autres risques digitaux. Cela impliquera des audits réguliers, des contrôles de conformité et des rapports plus rigoureux aux organismes de réglementation. L'amélioration de la gestion des risques deviendra une nécessité, car le règlement DORA impose une approche globale et intégrée de l'identification et de l'évaluation des risques associés aux services commerciaux et aux systèmes digitaux essentiels. Les entités financières devront mettre en place des contrôles solides et surveiller et atténuer ces risques en permanence. Pour de nombreuses entités financières, la mise en conformité avec le règlement DORA nécessitera des investissements technologiques plus importants.

Les entités financières devront investir dans des technologies avancées, telles que l'IA et le ML, pour améliorer et accélérer leur résilience opérationnelle et leurs capacités de réponse en fournissant une meilleure détection des menaces, des réponses automatisées et des analyses prédictives. Il sera également crucial de mettre l'accent sur la gestion des risques liés aux tiers. Les entités financières doivent s'assurer que leurs fournisseurs de services tiers ont mis en place de solides mesures de résilience opérationnelle. Cela implique de procéder à une diligence raisonnable approfondie, d'effectuer des évaluations régulières et d'établir des obligations contractuelles claires pour se protéger contre les risques digitaux. Le règlement DORA exige également une plus grande transparence. Les entités financières devront faire preuve d'une plus grande transparence quant à leurs pratiques en matière de résilience opérationnelle, en démontrant leur capacité à répondre efficacement aux perturbations digitales, en conservant des dossiers complets et en communiquant ouvertement avec les régulateurs, les parties prenantes et les clients.

L'importance du règlement DORA pour les entités financières

Le règlement DORA arrive à un moment crucial pour les entités financières, face à la fréquence et à la sophistication croissantes des cybermenaces. Selon le Fonds monétaire international, le secteur des services financiers a été, au cours des vingt dernières années, l'une des cibles les plus attrayantes pour les cybercriminels. Le montant des pertes a plus que quadruplé depuis 2017 pour atteindre 2,5 milliards de dollars, et les pertes indirectes telles que les atteintes à la réputation ou les mises à niveau de la sécurité sont nettement plus élevées. Les attaques ont non seulement compromis des informations financières sensibles, mais ont également posé des risques importants pour la stabilité et l'intégrité globales des systèmes financiers. Comme les entités financières dépendent de plus en plus de l'infrastructure digitale, la complexité et l'interconnexion de leurs systèmes les rendent plus vulnérables aux cybermenaces. Les attaquants exploitent ces vulnérabilités, en utilisant souvent des techniques sophistiquées telles que le déplacement latéral au sein des réseaux pour accéder à des données précieuses ou perturber les services. Cette méthode permet aux cybercriminels de passer d'un système à l'autre, ce qui rend difficiles la détection et la prévention des activités malveillantes, augmentant ainsi le risque de brèches importantes ou de perturbations opérationnelles.

L'adoption du règlement DORA est une réponse proactive à ces menaces en constante évolution. En établissant un cadre harmonisé pour la résilience numérique dans les États membres de l'UE, DORA vise à garantir un niveau cohérent de sécurité et de résilience opérationnelle dans l'ensemble du secteur financier. Cette uniformité est cruciale, car elle renforce la confiance dans l'infrastructure digitale du secteur, garantissant que les entités financières peuvent résister aux perturbations technologiques (et s'en remettre). La nature proactive du règlement DORA reflète un changement stratégique qui consiste à ne plus se contenter de réagir aux incidents, mais à anticiper et à atténuer les risques potentiels avant qu'ils ne se matérialisent. Cette approche vise non seulement à protéger les entités individuelles, mais aussi à préserver l'écosystème financier dans son ensemble des risques systémiques. L'accent mis par le règlement sur le renforcement des mécanismes de réponse aux incidents et sur l'amélioration de la gestion des risques par les tiers souligne l'importance d'une approche globale et intégrée de la cybersécurité.

La transparence est un autre aspect essentiel du règlement DORA. Les entités financières doivent fournir une plus grande visibilité sur leurs pratiques en matière de résilience opérationnelle, démontrant ainsi leur capacité à répondre efficacement aux perturbations digitales. Cette transparence est essentielle pour maintenir la confiance des régulateurs, des parties prenantes et des clients, et elle souligne l'engagement de l'institution à protéger son infrastructure digitale. L'importance du règlement DORA va au-delà de la conformité réglementaire. Ce règlement représente en effet un changement fondamental dans la manière dont les entités financières abordent la cybersécurité et la résilience opérationnelle. En s'alignant sur les exigences du règlement DORA, les entités financières se protègent non seulement contre les menaces actuelles et futures, mais se positionnent également comme des entités de confiance dans un paysage financier de plus en plus digital.

Comment Akamai aide les entités financières à se conformer au règlement DORA

En tirant parti de l'envergure de notre plateforme mondiale et de sa veille exhaustive sur les menaces, nous aidons les entités financières à prévenir, détecter et atténuer les cybermenaces dans les environnements sur site et dans le cloud, ce qui leur permet de faire face à la complexité de l'évolution des obligations réglementaires de conformité. Nos solutions permettent de répondre à chacun des piliers clés du règlement DORA (gestion des risques, notification des incidents, tests de résilience opérationnelle numérique, gestion des risques liés aux TIC pour les tiers et partage d'informations et de renseignements) garantissant une couverture complète et des postures de cybersécurité robustes.

API Security

Akamai API Security offre des fonctionnalités complètes de détection des API, de gestion des postures et de protection d'exécution basée sur l'IA/le ML, essentielles pour détecter et bloquer les attaques avancées par API en temps réel. Les tests de sécurité proactifs et les analyses en temps réel permettent aux entités financières d'auditer rapidement le comportement de l'API, de répondre aux menaces et de protéger les données sensibles, afin de se conformer aux exigences du règlement DORA en matière de gestion des risques liés aux TIC et de signalement des incidents.

L'atténuation des risques associés aux API fantômes, aux API vulnérables et aux abus d'API constitue un défi de taille en raison d'un manque de visibilité et de surveillance. Une sécurité efficace des API offre une découverte et un catalogage complets, une détection des menaces en temps réel et des mécanismes de protection pilotés par l'IA, garantissant une surveillance et une atténuation continues des menaces liées aux API et soutenant la conformité avec les normes du règlement DORA.

Akamai Guardicore Segmentation

Akamai Guardicore Segmentation permet aux entités financières de diviser leurs réseaux en segments sécurisés, réduisant ainsi considérablement le risque de mouvements latéraux des cybermenaces. Cette technologie s'aligne sur les objectifs du règlement DORA en améliorant la gestion des risques liés aux TIC et les tests de résilience opérationnelle numérique. En isolant les actifs compromis et en limitant les mouvements latéraux des adversaires, la microsegmentation contribue à maintenir une posture de sécurité solide et facilite une réponse efficace aux incidents.

Akamai Guardicore Segmentation offre une visibilité approfondie des dépendances applicatives et une application précise des règles, garantissant une gestion continue des règles de microsegmentation. La plateforme prend en charge les options de déploiement avec et sans agent, offrant ainsi une flexibilité pour divers environnements, notamment les environnements PaaS dans le cloud, IoT et OT. En s'appuyant sur la création de règles pilotée par l'IA et sur des flux de travail intuitifs, Akamai Guardicore Segmentation simplifie le processus de microsegmentation, permettant aux entités financières de mettre en œuvre et d'adapter rapidement les règles de sécurité à l'évolution des conditions du réseau. Cette approche globale permet non seulement de réduire la surface d'attaque, mais aussi de prendre en charge la conformité aux exigences réglementaires en matière de résilience opérationnelle numérique.

Edge DNS

Akamai Edge DNS garantit la haute disponibilité et les performances des services DNS, en protégeant les infrastructures DNS sur site, dans le cloud et hybrides. Cette solution est essentielle au maintien de la continuité des services et à la protection contre les cybermenaces à grande échelle, répondant aux exigences du règlement DORA en matière de gestion des risques TIC et de signalement des incidents.

App & API Protector

Akamai App & API Protector combat les attaques de couche 7 avec des protections complètes, notamment contre les dénis de service distribués (DDoS), les bots et les 10 principales exploitations selon l'OWASP. Cette solution prend en charge une sécurité robuste pour les applications Web et les API, ce qui est essentiel pour se conformer aux obligations de gestion des risques TIC et de signalement des incidents du règlement DORA.

Client-Side Protection & Compliance

Akamai booste votre conformité PCI et protège vos sites Web contre les attaques JavaScript. Cela permet de protéger les données sensibles des clients et d'aider les entités financières à répondre aux exigences strictes de conformité définies par le règlement DORA et d'autres réglementations.

Prolexic

Akamai Prolexic protège l'infrastructure contre les attaques DDoS. Cette plateforme offre des mécanismes de défense robustes pour garantir la disponibilité et la fiabilité, même lors d'attaques à grande échelle, soutenant ainsi les objectifs du règlement DORA d'améliorer la résilience opérationnelle numérique et les capacités de réponse aux incidents.

Bot Manager

Akamai Bot Manager offre une gestion avancée des bots conçue pour détecter et atténuer les bots malveillants sophistiqués tout en autorisant les bons bots. Cela permet de soutenir le trafic légitime, de maintenir une expérience utilisateur fluide et d'aider les entreprises à respecter les exigences du règlement DORA en matière de gestion des risques liés aux TIC.

Account Protector

Akamai Account Protector détecte et atténue le piratage et l'usurpation de comptes ainsi que le credential stuffing. Cette capacité est essentielle pour protéger les comptes des clients et maintenir la confiance, conformément à l'accent mis par le règlement DORA sur une gestion robuste des risques TIC et sur le signalement des incidents.

Content Protector

Akamai Content Protector empêche les extracteurs de voler du contenu et de réduire les taux de conversion. Cette solution permet de sécuriser les contenus propriétaires, ce qui va dans le sens des objectifs du règlement DORA en matière de protection des actifs digitaux et d'amélioration de la résilience opérationnelle.

Exigences détaillées et solutions Akamai

Gouvernance et organisation

Gouvernance de la sécurité : le centre de commande des opérations de sécurité d'Akamai fournit des services de surveillance et de réponse 24 h/24, 7 j/7, ce qui permet de contrôler en permanence la gouvernance de la sécurité.

Intégration de gestion des informations et des événements de sécurité (SIEM) : la solution d'intégration SIEM d'Akamai permet de diffuser les événements SIEM vers des outils d'analyse tels que Splunk, QRadar et ArcSight, ce qui vous permet d'incorporer les événements de sécurité d'Akamai dans votre infrastructure globale d'événements et de sécurité.

Gouvernance, risque et conformité (GRC) : l'Akamai Control Center fournit une interface centralisée pour la gestion des produits et services d'Akamai, offrant aux entreprises l'accès, les informations et le contrôle nécessaires pour les aider à répondre aux exigences en matière de risques, de conformité et de réglementation tout en offrant des expériences en ligne optimales.

Cadre de gestion des risques liés aux TIC

Logiciel de gestion des risques : Akamai Secure Internet Access offre une protection avancée contre les menaces, notamment contre les logiciels malveillants et l'hameçonnage.

Plateformes de protection des points de terminaison : Akamai Bot Manager permet de gérer et d'atténuer le trafic des robots malveillants.

Outils de gestion des failles de sécurité : les solutions d'Akamai permettent une analyse continue et une évaluation des vulnérabilités des systèmes TIC.

Gestion des incidents liés aux TIC

Plateformes de réponse aux incidents : les services de réponse aux incidents d'Akamai automatisent et orchestrent les processus de réponse aux incidents.

Systèmes de suivi des incidents : les solutions d'Akamai permettent de suivre et de gérer les rapports d'incidents et leurs résolutions.

Tests de résilience opérationnelle numérique

Services de test de pénétration : Akamai propose un service client intégré de tests d'intrusion et d'autres services d'évaluation de la sécurité.

Exercices équipe rouge/équipe bleue : Akamai organise régulièrement des exercices de sécurité afin d'évaluer et d'améliorer la réponse de l'organisation et d'assurer la conformité aux réglementations.

Gestion des risques par des tiers

Plateformes de gestion des risques par des tiers : les produits de sécurité d'Akamai, notamment le pare-feu d'application web (WAF) et la passerelle d'API, contribuent à la gestion et à l'atténuation des risques.

Logiciel de gestion des contrats : les solutions d'Akamai permettent de gérer les obligations contractuelles et de garantir la conformité.

Plateformes de veille sur les menaces : les services de veille sur les menaces d'Akamai fournissent des informations actualisées sur les menaces émergentes à l'aide de flux externes et internes.

FS-ISAC (Financial Services Information Sharing and Analysis Center, ou Centre d'analyse et de partage des informations des services financiers) : Akamai est le membre fondateur du programme de fournisseur critique FS-ISAC. La collaboration interne et le partage de renseignements sur les menaces restent essentiels pour sécuriser avec succès l'infrastructure du secteur des services financiers grâce à une communication rapide sur les vulnérabilités, les pannes, les risques ou les violations. Notre accès unique aux données relatives au trafic et aux attaques nous permet de nous associer à la recherche et de faire part des meilleures pratiques aux membres.

Surveillance et mise en œuvre

Outils d'audit et de conformité : les solutions de conformité d'Akamai permettent d'auditer et de garantir le respect des exigences réglementaires.

Solutions de surveillance et de création de rapports : le Control Center offre des fonctionnalités complètes de surveillance et de création de rapports.

Références clients démontrant l'efficacité d'Akamai

Pour déterminer si Akamai est apte à contribuer à la conformité réglementaire, l'examen des expériences des clients peut s'avérer très instructif. Voici quelques cas pertinents :

Grande compagnie d'assurance : ce témoignage montre comment cet assureur exploite les solutions d'Akamai pour améliorer la sécurité et les performances. Les offres d'Akamai permettent d'atténuer les attaques DDoS et de sécuriser les API, qui sont des éléments cruciaux pour maintenir la gestion des risques TIC et la réponse aux incidents, comme l'exige le règlement DORA.

CashFlows : CashFlows utilise les solutions de sécurité d'Akamai pour protéger sa plateforme de paiement hébergée dans le cloud. Ce cas démontre comment Akamai aide à maintenir la conformité aux normes de sécurité et à se protéger contre les menaces telles que les attaques DDoS, en assurant une disponibilité et une sécurité continues des services de paiement. Cette technologie s'aligne sur les exigences du règlement DORA en améliorant la gestion des risques liés aux TIC et les tests de résilience opérationnelle numérique.

LANDBANK : en tant que plus grande banque publique des Philippines, LANDBANK s'appuie sur Akamai pour sécuriser ses applications en ligne, se protéger contre les cybermenaces et simplifier sa transformation digitale. Cette histoire est particulièrement pertinente pour comprendre comment les solutions d'Akamai peuvent aider à gérer les risques liés aux tiers et à garantir des processus robustes de gestion des incidents.

Ces exemples illustrent la manière dont les solutions de sécurité complètes et les capacités de gestion proactive des menaces d'Akamai peuvent aider les entités financières à répondre aux exigences du règlement DORA, notamment en ce qui concerne la gestion des risques liés aux TIC, le signalement des incidents, les tests de résilience opérationnelle numérique et la gestion des risques liés aux tiers.

Conclusion

Le règlement DORA représente un changement significatif dans le paysage réglementaire des entités financières, exigeant des mesures de cybersécurité complètes et proactives. La suite de solutions d'Akamai offre un cadre solide aux entités financières pour les aider (1) à répondre aux exigences strictes du règlement DORA et (2) à garantir une meilleure résilience opérationnelle numérique, une gestion solide des risques liés aux TIC et des capacités efficaces de réponse aux incidents. En exploitant les technologies avancées d'Akamai, les entités financières peuvent naviguer en toute confiance dans les complexités de la conformité DORA et protéger leurs opérations contre l'évolution de l'écosystème des menaces.

Apprenez-en plus sur nos solutions pour les services financiers

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure et de la visibilité de notre plateforme mondiale, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision.

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Akamai Connected Cloud, plateforme cloud massivement distribuée en bordure de l'Internet, rapproche les expériences et les applications des utilisateurs tout en éloignant les menaces. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 09/24.