DORA : une révolution réglementaire pour la cybersécurité des entités financières

La directive DORA, Digital Operational Resilience Act, entrera en vigueur en janvier 2025. Elle imposera aux institutions financières, et notamment aux fonds d'investissement, des exigences strictes pour renforcer leur cybersécurité.

Temps de lecture : minute

27 novembre 2024

La directive DORA (Digital Operational Resilience Act) est une nouvelle réglementation de l'Union européenne destinée à renforcer la résilience opérationnelle numérique des entités financières face aux cybermenaces. Elle fait partie d'un ensemble plus large de mesures visant à protéger le secteur financier des risques liés à la cybersécurité et aux perturbations numériques. DORA a été adoptée par les institutions de l'UE en décembre 2022, et son entrée en vigueur est prévue pour le 17 janvier 2025.

Cette directive impose aux institutions financières, et notamment aux fonds d'investissement, des exigences strictes pour renforcer leur cybersécurité. Elle oblige ces entités à mieux gérer les risques liés aux technologies de l'information et de la communication (TIC) en mettant en place des mécanismes de surveillance continue de leurs systèmes. L'objectif est de mieux prévenir et détecter les cyberattaques et incidents de sécurité, afin d'assurer une protection plus efficace du secteur financier.

Des exigences de conformité fortes, mais adaptées aux différentes entités financières

« En accompagnant les entreprises dans leur mise en conformité, on constate que cette réglementation amène des changements profonds dans la façon dont elles perçoivent et gèrent leurs risques cyber », explique Thomas Hutin, directeur de l'équipe Cyber chez FTI Consulting. *« Ce n'est pas seulement une question de conformité, mais une véritable réponse à des menaces bien réelles »*, poursuit-il.

Le cadre imposé par DORA est ambitieux et couvre un large spectre de mesures, de la surveillance continue des systèmes à la gestion des prestataires tiers, en passant par la mise en place de plans de réponse aux incidents. Les entités doivent également se préparer à documenter et reporter tout incident cyber de manière rigoureuse et dans des courts délais. *« Cette réglementation est en ligne avec les bonnes pratiques du domaine, mais son application exige une compréhension profonde des risques et une intégration des enjeux cybersécurité dans les plus hautes instances décisionnelles »*, précise Thomas Hutin.

D'après lui, les grandes banques se préparent depuis longtemps, mais il semblerait que d'autres acteurs, notamment certains VC et fintechs, soient moins en avance sur ce sujet de mise en conformité. Heureusement, si DORA impose des exigences transversales à toutes les institutions financières, elle prévoit une certaine flexibilité selon les ressources et les risques spécifiques à chaque type d'entité. *« Dans la mise en application de cette directive, le principe de proportionnalité est essentiel. On ne demande pas les mêmes efforts à une grande banque systémique qu'à un fonds d'investissement »*, avance-t-il.

« Cependant, l'enjeu est de taille pour chacun : la cybersécurité devient un prérequis pour conserver la confiance des clients et des partenaires », ajoute Thomas Hutin. Pour les fintechs et autres acteurs innovants,

l’approche “sécurité by design” s’impose. *« Il est crucial pour eux d’intégrer les principes de sécurité dès la conception de leurs services pour éviter plus tard des surcoûts et des vulnérabilités additionnelles à long terme »*, conclut Thomas Hutin.

À lire aussi
Maddyness lance MDVC, une plateforme pour tout savoir sur les fonds d’investissement

Article écrit par Manon Triniac