Guide pour comprendre le règlement sur la résilience opérationnelle numérique

(Digital Operational Resilience Act)

Barracuda

Le Digital Operational Resilience Act (DORA) est un règlement de l'Union européenne (UE) qui entrera en vigueur le 17 janvier 2025 et qui vise à renforcer la résilience des institutions financières en matière de cybersécurité.

La législation marque un changement fondamental dans la manière dont le public et les autorités de régulation perçoivent la cybersécurité et la transparence des entreprises. Elle reconnaît que les entreprises ne doivent pas négliger leur propre défense et que le fait d'être parfaitement conscient des infractions assure une plus grande sécurité pour l'ensemble de la société.

Le règlement DORA reconnaît que le secteur des services financiers dépend de plus en plus de l'infrastructure numérique et de l'importance de sécuriser cette infrastructure. Il représente les meilleures pratiques, exigeant des entreprises qu'elles mettent en place des pratiques résilientes et qu'elles signalent les violations et les dysfonctionnements rencontrés.

La législation intègre l'idée qu'une attaque réussie contre une infrastructure financière numérique pourrait causer des dommages à l'ensemble de la société. Une cyberattaque peut avoir des effets sur le long terme car il faut du temps et de l'argent pour faire face et trouver une solution. Les cybercriminels et les acteurs soutenus par l'État ont accès à des outils d'attaque de plus en plus sophistiqués et automatisés. La sécurité numérique n'est donc plus une option, mais une obligation pour les entreprises.

Ce livre électronique présente le règlement DORA ainsi que les différentes sources d'information et les meilleures pratiques à adopter pour se mettre en conformité avec celui-ci. Il identifie également les ressources Barracuda qui peuvent vous aider à vous préparer pour la mise en œuvre de ces pratiques.

Barracuda

Qui est concerné par le règlement DORA ?

Le règlement DORA s'applique à la plupart des institutions financières, notamment :

- Les banques, les compagnies d'assurance, les entreprises d'investissement et les établissements de crédit
- Les prestataires de paiement et les FinTechs
- Les gestionnaires d'actifs et les plateformes de trading

DORA couvre essentiellement toute entité impliquée dans le secteur financier qui utilise des technologies et des services de communication, ainsi que leurs fournisseurs de services TIC essentiels. Il couvre non seulement les entreprises de l'UE, mais également toutes les entreprises du monde entier qui exercent leurs activités ou ont des clients sur le territoire. Si les entreprises britanniques qui n'ont pas de clients dans l'UE ne sont pas tenues de se conformer au règlement DORA, le gouvernement britannique devrait créer son propre cadre réglementaire, qui sera probablement très proche de la réglementation européenne. Mais au-delà de la conformité, s'assurer que votre organisation est en accord avec les recommandations DORA signifie que vous suivez les meilleures pratiques modernes.

Quels sont les cinq éléments clés du règlement DORA ?

L'objectif global du règlement DORA consiste à renforcer la résilience opérationnelle des institutions financières face aux cyberattaques tout en harmonisant les règles au sein de l'UE. Le règlement comporte cinq principaux éléments :

Gestion des risques : les institutions financières doivent mettre en œuvre de solides procédures de gestion des risques informatiques. Il s'agit notamment de procédures d'identification, d'évaluation et d'atténuation des risques potentiels liés à leurs systèmes informatiques, à leurs systèmes dans le Cloud et à leurs réseaux de la chaîne d'approvisionnement.

Test de résilience : le règlement DORA reconnaît qu'aucune mesure de sécurité n'est fiable si elle n'est pas testée. Les institutions financières doivent donc disposer d'un plan de réponse aux incidents adéquat et avoir des employés qui en comprennent le fonctionnement. Ces institutions doivent régulièrement tester la solidité de leur infrastructure numérique contre les perturbations de fonctionnement, par exemple au moyen de tests de pénétration, de tests de résistance et d'évaluations de la vulnérabilité.

Notification d'incidents : procédez à des évaluations complètes des risques et mettez en œuvre des politiques solides en matière de sécurité des systèmes d'information. Cela vous permettra de mettre en place une approche proactive pour identifier et atténuer toute menace potentielle. Établissez des processus de réponse aux incidents, effectuez des simulations et formez vos employés pour qu'ils soient prêts.

Gestion des risques liés aux tiers : le règlement DORA reconnaît également le danger des attaques dans la chaîne d'approvisionnement. Il exige des institutions financières qu'elles surveillent les fournisseurs de services tiers, notamment les fournisseurs de services tels que les sociétés de Cloud. Ces institutions doivent conclure des accords écrits avec leurs fournisseurs qui abordent les sujets mentionnés à l'article 30 du règlement DORA, tels que disposer d'une description écrite de tous les services fournis et, le cas échéant, des engagements en matière de niveau de service.

Partage d'informations : le règlement vise à harmoniser les obligations de notification au sein de l'UE et à renforcer le dispositif de sécurité de l'ensemble du secteur en encourageant une meilleure coopération et un meilleur partage des informations entre les entreprises. Cela implique l'obligation de signaler rapidement les incidents après qu'ils se sont produits. Auparavant, cela se faisait de manière ad-hoc et non transparente.

Conformité et mise en application

Il est possible que vous trouviez que le règlement DORA ne s'écarte pas radicalement des meilleures pratiques établies. Cette hypothèse est juste. Cependant, ce qui est différent avec le règlement DORA, c'est qu'il exigera des institutions qu'elles prouvent qu'elles font effectivement ce qu'elles doivent faire. Il n'existe pas de certification ou de test de conformité unique, mais le règlement DORA ajoutera une charge de gouvernance et de documentation à de nombreuses entreprises. La mise en œuvre sera du ressort des trois organismes de régulation financiers actuels de l'UE, les autorités européennes de surveillance.

Sanctions

Les organismes de régulation ont le pouvoir discrétionnaire d'imposer des sanctions aux organisations qui ne se conforment pas au règlement. Les États membres ont également la possibilité d'imposer des sanctions pénales.

Quelles sont les premières étapes à suivre pour se conformer au règlement DORA ?

La première tâche consiste à déterminer si le règlement DORA s'applique directement à votre entreprise. Comme indiqué précédemment, même si cela ne s'applique pas directement, les institutions financières doivent tenir compte de l'ensemble raisonnable de bonnes pratiques en matière de cybersécurité contenues dans le règlement DORA. Si vos projets de croissance impliquent une expansion dans l'UE ou des activités avec des institutions financières opérant au sein de l'UE, nous vous conseillons de vous mettre en conformité dès maintenant. Si vous devez vous mettre en conformité d'ici le mois de janvier, vous devrez agir rapidement et, le cas échéant, demander une aide extérieure. Si vous fournissez des services à des entreprises de l'UE actives dans le secteur des services financiers, vous devez travailler en étroite collaboration avec elles afin d'aligner vos stratégies.

La deuxième étape consiste à effectuer une analyse des lacunes afin de mesurer le degré de maturité de votre système de cybersécurité et de déterminer dans quelle mesure vos systèmes correspondent à ceux exigés par le règlement. Une fois cette étape effectuée, vous pourrez commencer à combler les lacunes et à mettre en place le personnel, les processus et la technologie nécessaires.

Barracuda

En savoir plus

L'Autorité européenne des assurances et des pensions professionnelles propose un guide destiné aux entreprises pour comprendre le règlement DORA. Si vous avez besoin d'informations supplémentaires, vous pouvez consulter la législation actuelle (PDF de 75 pages).

Barracuda Networks peut aider votre organisation à se conformer aux cinq composantes principales du règlement DORA. Notre suite complète d'outils de cybersécurité peut renforcer votre dispositif de sécurité dans tous les domaines, du courrier électronique aux applications web, en passant par la sécurité du réseau.

Nous disposons d'un large éventail de ressources en ligne pour vous aider à appliquer le règlement DORA, notamment pour utiliser XDR afin d'améliorer votre détection et votre réponse aux menaces, et obtenir l'approbation pour vos stratégies en matière de cybersécurité.

Nous pouvons également vous aider à affiner votre réponse aux incidents. Enfin, Barracuda Security Insights peut vous aider à fournir l'intelligence active dont vous avez besoin pour effectuer votre analyse des risques.

Barracuda en quelques mots

Notre mission est de renforcer la sécurité de tous. Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité de niveau professionnel cloud-first, abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients, et de se développer en conséquence. Plus de 200 000 entreprises partout dans le monde ont choisi Barracuda pour veiller à leur sécurité pendant qu'elles prospèrent. Pour en savoir plus, rendez-vous sur fr.barracuda.com.