Réglementation DORA : ce que vous devez savoir

Vie privéeConformité en matière de sécurité

13 novembre 2023 Temps de lecture : 5 min

Le secteur des services financiers a toujours été enthousiaste à l'idée d'adopter des innovations technologiques, c'est pourquoi au cours des 10 dernières années, il a changé presque au point d'être méconnaissable. Les clients utilisent désormais des applications mobiles et de bureau pour les opérations bancaires, les investissements, les assurances, la fiscalité, etc., mais l'infrastructure TIC (Technologie de l'Information et de la Communication) nécessaire pour prendre en charge toute cette livraison numérique introduit un grand nombre de points de défaillance potentiels ainsi que des voies d'attaque. Cela rend les fournisseurs de services financiers individuels, et le système dans son ensemble, potentiellement très vulnérables.

L'Union européenne s'est rendu compte que si des événements tels que des guerres, des catastrophes naturelles ou des cyberattaques parvenaient à paralyser le secteur financier européen, les conséquences seraient désastreuses.

Loi sur la résilience opérationnelle numérique (DORA).

Cette nouvelle loi est entrée en vigueur le 16 janvier 2023 et les organisations qu'elle couvre devront répondre à ses exigences à partir du 17 janvier 2025.

À qui DORA s'applique-t-il ?

DORA s'applique aux 22 000 entités financières européennes, ainsi qu'aux fournisseurs d'infrastructures TIC qui leur permettent de fonctionner. Les entreprises qui devront améliorer leur gestion des risques et leur cybersécurité d'entreprise sur la base de DORA sont les suivantes :

· Banques

· Etablissements de crédit

· Agences d'évaluation du crédit

· Fournisseurs de services d'information sur les comptes

· Caisses de pension

· Entreprises de crypto-monnaies

· Entreprises d'investissement

· Fournisseurs d'assurance

· Fournisseurs de financement participatif

· Gestionnaires de fonds d'investissement alternatifs

· Intermédiaires

· Prestataires de services TIC

Comme son nom l'indique, la loi a pour principal objectif de renforcer leur *Résilience opérationnelle numérique* afin que les marchés financiers et les services évitent des perturbations majeures et continuent de fonctionner sans heurts si des événements catastrophiques devaient encore se produire.

Il est important de noter que, même si ces fournisseurs d'infrastructures se trouvent dans des territoires situés en dehors de l'UE, mais qu'ils desservent des entreprises qui y sont présentes, ils devront satisfaire à certaines exigences de la DORA. Le niveau de surveillance qu'ils suscitent et les exigences

qu'ils doivent remplir varieront en fonction du niveau de risque, mais cela signifie que les entreprises fournissant des services de cloud computing ou des fournisseurs de pixels de suivi aux fournisseurs financiers de l'UE devront se conformer aux exigences de la loi.

La réglementation DORA est composée de cinq « piliers » clés qui sont :

1. **Gestion des risques liés aux TIC** : Ce pilier met l'accent sur les responsabilités du conseil d'administration dans l'élaboration et l'approbation de la Stratégie de résilience opérationnelle numérique (DORS). Il s'agit notamment de créer des politiques visant à protéger la confidentialité, l'intégrité et la disponibilité de toutes les données, d'assurer la communication, la coopération et la coordination par la mise en œuvre d'un cadre de gouvernance des TIC et d'utiliser des solutions TIC pour prévenir les violations de la confidentialité, l'atteinte à l'intégrité, le manque de disponibilité et la perte de données.

2. **Signalement des incidents liés aux TIC** : souligne la nécessité d'une stratégie de communication pour la divulgation des incidents liés aux TIC dans le cadre de la stratégie de résilience opérationnelle numérique (DORS). DORA s'efforce de rationaliser le processus de signalement, en encourageant une enquête et une réponse rapides aux violations afin d'en réduire l'impact.

3. **Tests de résilience opérationnelle numérique** : les entreprises devront mettre en œuvre des programmes d'évaluation des tests qui, par nécessité, impliqueront probablement l'utilisation d'outils automatisés pour identifier et corriger les problèmes avant qu'ils ne puissent menacer les opérations.

4. **Gestion des risques liés aux tiers** : traite de la gestion des risques associés aux fournisseurs de services TIC tiers.

5. **Partage de l'information et du renseignement** : met l'accent sur l'élaboration de processus d'échange d'information sur les cybermenaces. De nombreux auteurs de menace ciblant le secteur financier tenteront de cibler plusieurs organisations simultanément. DORA encourage les organisations à partager des renseignements sur les menaces avec leurs pairs afin d'améliorer la sensibilisation à l'évolution des cybermenaces.

Réglementation DORA – Par où commencer ?

L'objectif principal de DORA est de s'assurer que les sociétés financières surveillent systématiquement la sécurité et les outils TIC afin de minimiser les risques. Ils devront adopter une approche proactive de la gestion des risques en examinant continuellement leurs mesures de sécurité et les niveaux de risque liés aux tiers. Le meilleur point de départ sera un examen des articles de DORA et un examen de la situation actuelle de l'entreprise.

À partir de là, ils devront travailler sur des stratégies visant à minimiser les risques opérationnels, mettre en place des réponses planifiées à l'avance pour faire face aux menaces de sécurité et s'engager à investir continuellement dans de nouveaux outils, politiques et procédures. L'objectif est la résilience continue, c'est pourquoi la mesure des indicateurs clés de performance en matière de sécurité sera un engagement permanent.

Proportionnalité

Les cinq piliers sont composés de 64 articles qui décrivent en détail les exigences. Comme l'article 4 l'indique, les attentes en matière de respect des exigences seront appliquées proportionnellement au profil de risque du fournisseur de TIC. Par exemple, si des dizaines d'entreprises financières s'appuyaient toutes sur le même fournisseur de services cloud, cela indiquerait un niveau de risque élevé, car en cas de défaillance, elles seraient toutes impactées. Ainsi, ce fournisseur serait désigné comme un *Fournisseur tiers de TIC critique et, e*n plus d'avoir à maintenir la conformité, il serait également soumis à une surveillance directe de la part des régulateurs financiers européens.

Pénalités DORA

DORA permet à ses superviseurs principaux d'imposer des pénalités de non-conformité aux organisations. Ces amendes peuvent représenter jusqu'à 1 % de leur chiffre d'affaires quotidien moyen dans le monde au cours de l'exercice précédent et être émises périodiquement pendant six mois maximum jusqu'à ce qu'elles soient conformes à la loi.

Sites Web des fournisseurs de services financiers

Nous étions impatients de comprendre comment tout cela serait lié à la mise à disposition du site Web d'un fournisseur de services financiers européen, nous nous sommes donc entretenus avec le PULSEC Group, un fournisseur de services de conseil, pour obtenir son avis d'expert.

Ils ont attiré notre attention sur le paragraphe 7 de l'article 3, qui définit un actif TIC comme suit : *"... un actif logiciel ou matériel dans le réseau et les systèmes d'information utilisés par l'entité financière.*

Un site web et les éléments qui le sous-tendent relèvent clairement de la rubrique « actifs TIC » et, en vertu de cette définition, ils comportent également des risques conformément au paragraphe 18 de l'article 3. Elle définit un « risque lié aux tiers dans le domaine des TIC » comme un *"... risque pouvant survenir pour une entité financière en relation avec son utilisation des services TIC fournis par des prestataires de services tiers ou par des sous-traitants de ces derniers, y compris par le biais d'accords d'externalisation.*

Le groupe PULSEC nous a dit que tous les composants qui entrent dans la construction d'un site Web sont sous le coup de la loi, y compris les éléments tiers tels que les outils d'analyse, les pixels et autres solutions SaaS. Ainsi, pour les prestataires de services financiers ayant des liens avec l'UE, ces définitions placent leurs sites Web et les fournisseurs de logiciels tiers sur lesquels ils s'appuient dans le champ d'application de DORA.

Gérer les risques avec Reflectiz

Reflectiz a un rôle clé à jouer pour garantir que les prestataires de services financiers ayant des liens européens restent conformes à DORA.

L'article 10, paragraphe 1, qui relève du pilier gestion des risques, dit :

« Les entités financières doivent mettre en place des mécanismes pour détecter rapidement les activités anormales, conformément à l'article 17, y compris les problèmes de performance des réseaux TIC et les incidents liés aux TIC, et pour identifier les points de défaillance uniques importants potentiels. »

Reflectiz est l'un de ces mécanismes. Elle contribue à la résilience opérationnelle d'une organisation en scannant en continu tous les composants connectés à ses sites web pour *activités anormales,* révélant :

· Quels composants de première, troisième, quatrième et n partie sont connectés au site. Les exemples incluent Google Analytics, CRM, WordPress, Pixels Facebook etc.

· les comportements de collecte de données ou de suivi actif de chaque composant.

· avec quels domaines les composants communiquent. Le système peut rapidement détecter et signaler les activités suspectes et malveillantes, y compris lorsque des composants tentent d'envoyer des données en dehors de l'UE.

Reflectiz commence par cartographier et maintenir un inventaire accessible de tous les actifs numériques connectés à un site Web et établit une base de référence pour leurs comportements. Cette approche automatisée permet de maintenir une visibilité à la minute près de ces actifs connectés, ce qui est essentiel pour la sécurité, et est également particulièrement utile pour la collecte de preuves, aidant ainsi les entreprises à se conformer aux exigences de déclaration obligatoire de DORA.

À un peu plus d'un an de la mise en œuvre, il est important que les fournisseurs de services financiers mettent en place dès maintenant leurs mesures de **résilience opérationnelle**. Reflectiz peut être un élément clé pour renforcer le profil de résilience opérationnelle de votre entreprise et répondre à ses responsabilités en vertu de DORA, alors ne tardez pas :

Demandez une présentation - démonstration.

Relfectiz est distribué en France par AMC SOFT
https://amcsoft.fr Email : contact@amcsoft.fr Tel : +33680741316