capitalfinance

PAYS : France
PAGE(S) :1;14;15
SURFACE :160 %
PERIODICITE : Hebdomadaire

RUBRIQUE : Premiere page
JOURNALISTE : Delphine Iweins

► **13 mai 2024**

DROIT

DORA ET LE RISQUE CYBER

Le règlement européen impose de nouvelles précautions aux dirigeants du secteur financier.

P. 14

DOSSIER

capitalfinance

PAYS :France
PAGE(S) :1;14;15
SURFACE :160 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Premiere page
JOURNALISTE :Delphine Iweins

► 13 mai 2024

Dora rend les dirigeants responsables de toute négligence informatique

Le règlement européen Dora impose aux acteurs financiers de constituer une gouvernance dédiée aux risques cyber en repensant leurs contrats avec les prestataires de technologies de l'information.

PAR **DELPHINE IWEINS**

La transformation numérique a un revers. Elle augmente l'exposition des ressources des entreprises aux cyberattaques. Et le secteur financier n'est pas épargné. Une récente étude de Sophos montre que le nombre d'attaques de ransomwares dans le secteur financier a bondi de 64 % en 2023, soit près du double du niveau de 2021.

Face à l'accroissement du risque, le Parlement européen a constaté la nécessité de mettre en place des règles communes de sécurité numérique au secteur financier. C'est ainsi qu'est né le règlement Dora, entré en vigueur le 16 janvier 2023. Son objectif ? S'assurer de la résilience du secteur financier et de ses acteurs (banques, instituts de paiements électroniques, assurances, établissements cryptoactifs, etc.) en cas de cyberattaques afin qu'ils continuent de fonctionner. Ces derniers vont devoir identifier, prévenir et réduire ces risques par une gouvernance dédiée, des formations et des dispositifs contractuels avec leurs prestataires informatiques, sous peine de sanctions. « *Il ne faut pas oublier que la perspective de résilience est au bénéfice de la sécurité de l'entreprise* », rappelle Thomas Hutin, senior managing director, responsable France du département cybersécurité du cabinet de conseil FTI Consulting.

iStock

capitalfinance

PAYS :France
PAGE(S) :1;14;15
SURFACE :160 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Premiere page
JOURNALISTE :Delphine Iweins

► 13 mai 2024

> Certains acteurs du secteur financier n'ont pas réalisé l'importance et le périmètre de Dora. »
>
> **NICOLAS QUOY**
> **ASHURST**

Les obligations de Dora sont réunies dans quatre grands piliers : la gestion des risques, la résilience opérationnelle, la surveillance et la conformité. Les entreprises sont tenues de mettre en place une approche efficace pour gérer et minimiser les risques liés à la cybersécurité. Problème, le niveau de maturité diffère d'une organisation à l'autre et la menace cyber n'est pas toujours encore bien estimée par les organes dirigeants et les conseils d'administration. Aux entreprises donc d'identifier les dangers potentiels, d'évaluer leur impact et d'appliquer des mesures appropriées pour les modérer *« Il est nécessaire d'allouer du temps et des ressources pour suivre ces risques cyber dans la durée »*, conseille vivement Thomas Hutin.

UNE GOUVERNANCE DÉDIÉE

La sensibilisation au risque cyber concerne autant le conseil d'administration et autre organisme de direction, que les salariés et les prestataires informatiques. *« Dora rassemble dans une gouvernance dédiée. Celle-ci nécessite d'embarquer un certain nombre de départements de l'entreprise »*, confirme le senior managing director, responsable France du département cybersécurité de FTI Consulting. L'organe de direction a un rôle déterminant dans le pilotage de cette gestion des risques car elle veille, notamment, au respect d'une hygiène informatique rigoureuse.

D'après l'article 4 du règlement, la *« pleine responsabilité de l'organe de direction dans la gestion des risques informatiques de l'entité financière »* est un principe général qui se décline en une série d'exigences spécifiques, telles que *« l'attribution de rôles et de responsabilités clairs pour toutes les fonctions liées à l'informatique, un engagement continu dans le contrôle du suivi de la gestion des risques informatiques, ainsi que dans l'ensemble des processus d'approbation et de contrôle et une répartition appropriée des investissements et des formations dans le domaine informatique »*.

L'obligation pour les membres de la direction de disposer d'une formation spécifique pour comprendre et évaluer les menaces informatiques ainsi que leurs impacts sur les opérations est également mentionnée explicitement. Le régulateur s'attend à ce que ceux-ci développent et entretiennent leurs connaissances en matière de risques liés aux technologies de l'information et de la communication. Cette gouvernance se réalise à deux niveaux : une analyse des risques à l'échelle de l'entreprise et une analyse en fonction de ses applications. Tous les acteurs financiers doivent être capables de documenter et de montrer leur cartographie auprès des autorités de surveillance européennes. Ils doivent aussi tenir un registre des contrats conclus avec l'ensemble de leurs prestataires informatiques.

REPENSER SES CONTRATS

La priorité est donc de s'atteler à la mise à jour des contrats avec ses prestataires informatiques. En effet, le règlement Dora vise à garantir la capacité des entreprises à résister à et se remettre des incidents cyber. Il est indispensable de disposer de systèmes adéquats de détection et de réponses aux menaces, ainsi qu'un plan d'urgence solide pour minimiser les temps d'arrêt et continuer les activités. *« Certains acteurs du secteur financier n'ont pas réalisé l'importance et le périmètre de Dora par rapport à leurs prestataires technologies de l'information et de la communication (TIC), dont l'immense majorité est désormais incluse »*, constate Nicolas Quoy, associé du cabinet Ashurst. L'Autorité bancaire européenne proposait déjà aux entreprises des bonnes pratiques envers leurs prestataires, mais rien d'obligatoire. Le règlement européen est d'un autre niveau.

Dora introduit une notion de « risque lié aux prestataires tiers » et impose de nouvelles clauses contractuelles. Par exemple, le contrat du prestataire TIC doit déterminer par avance des frais d'assistance. Celui-ci doit aussi participer à des tests de pénétration pour s'assurer que le système d'information de l'entreprise cliente est correctement protégé. *« Le prestataire est inclus beaucoup plus en amont, en ce sens qu'il doit par exemple participer aux tests de pénétration et aux formations en matière de résilience réalisés par l'entité financière »*, explique l'avocat spécialiste de la digital economy. *« Ces tests se réalisent par le biais d'audits, de revues documentaires, des tests d'intrusion et de red team test c'est-à-dire avec les mêmes modes opératoires que les hackers »*, précise Thomas Hutin.

Les clauses les plus disputées vont porter sur l'audit des sous-traitants. En effet, en plus des formations et révisions contractuelles, les acteurs financiers ont aussi la responsabilité d'analyser le risque de criticité de leurs prestataires TIC. Ils disposeront d'un pouvoir de contrôle sur les sous-traitants utilisés par leurs prestataires. D'ailleurs, ces derniers sont obligés de demander à leurs clients l'autorisation de faire appel à des sous-traitants.

Une fois ces audits et tests réalisés, les prestataires informatiques seront rangés par leurs clients en deux catégories : ceux qui supportent des fonctions critiques importantes et les autres, plus classiques, qui auront de ce fait moins d'obligations contractuelles. *« Ces deux catégories feront l'objet d'interprétation. Il appartient aux acteurs financiers de décider à quelle catégorie appartiennent leurs prestataires informatiques, de les cartographier et de maintenir un registre d'informations des contrats correspondants »*, tempère Nicolas Quoy.

DES SANCTIONS ENCORE À DÉFINIR

Le règlement Dora demande de maintenir une résilience constante dans un contexte technologique de plus en plus complexe. Ce n'est pas un exercice de mise en conformité ponctuel, même si les délais pour atteindre ces objectifs sont assez courts.

En effet, les acteurs financiers ont jusqu'au 17 janvier 2025 au plus tard pour respecter ces nouvelles obligations. Cependant, les sanctions ne sont pas encore connues car le règlement européen ne les définit pas.

L'appréciation des sanctions est laissée aux Etats membres qui peuvent *« imposer des sanctions pénales »* et arrêter *« des règles prévoyant des sanctions administratives et des mesures correctives appropriées en cas de violation »* du règlement.

L'article 50 de Dora prévoit que ces sanctions *« sont effectives, proportionnées et dissuasives »*. Il pourra s'agir, par exemple, d'un système de named & shame, du retrait d'un agrément ou bien encore de fortes amendes. ■

CHIFFRES CLÉS

Dans leur rapport 2023 sur le paysage des fournisseurs tiers de TIC dans l'UE, les autorités européennes de surveillance dénombraient 15.000 prestataires de technologies de l'information et de la communication de l'information pour 1.600 entités financières en Europe.