Finance numérique: loi sur la résilience opérationnelle numérique (DORA)

2020/0266(COD) - 07/12/2021 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des affaires économiques et monétaires a adopté le rapport de Billy KELLEHER (Renew Europe, IE) sur la proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648 /2012, (UE) nº 600/2014 et (UE) nº 909/2014.

La proposition de la Commission relative à un acte législatif sur la résilience opérationnelle numérique du secteur financier (DORA) vise à définir des exigences uniformes concernant la sécurité des réseaux et des systèmes d'information en vue de mettre en place un cadre global qui améliorera la gestion des risques liés au numérique par les entités financières.

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Exigences uniformes

Les exigences applicables aux entités financières concerneront : i) la gestion des risques liés aux technologies de l'information et de la communication (TIC); ii) la notification, aux autorités compétentes, des incidents majeurs liés à l'informatique; iii) la notification aux autorités compétentes, par les établissements de crédit, les établissements de paiement et les établissements de monnaie électronique, des incidents opérationnels ou de sécurité majeurs liés au paiement; iv) les tests de résilience opérationnelle numérique; v) le partage d'informations et de renseignements en rapport avec les cybermenaces et les cybervulnérabilités; vi) les mesures destinées à garantir la gestion solide du risque lié aux tiers prestataires de services informatiques par les entités financières.

Le règlement serait sans préjudice des compétences des États membres concernant la préservation de la sécurité publique, de la défense et de la sécurité nationale.

Champ d'application

La proposition s'appliquerait aux intermédiaires d'assurance, **qui ne sont pas des micro, petites ou moyennes entreprises**, à l'exception des entreprises qui dépendent exclusivement de systèmes de vente automatisés organisés. Les contrôleurs légaux des comptes et les cabinets d'audit de petite et moyenne taille seraient également exclus du champ d'application du règlement, sauf cas exceptionnels. Le règlement s'appliquerait aux prestataires de **services informatiques intra-groupe**, à l'exception du cadre de supervision visé au chapitre V.

Principe de proportionnalité

Le texte amendé précise que les entités financières devront mettre en œuvre les règles introduites par les chapitres II (gestion des risques), III (gestion, classification et notification des incidents liés à l' informatique) et IV (tests de résilience) conformément au principe de proportionnalité, **en tenant compte de leur taille, de la nature, de l'ampleur et de la complexité** de leurs services, activités et opérations et de leur profil de risque global.

Le règlement ne s'appliquerait pas aux petites entreprises d'investissement non interconnectées, aux établissements de crédit et aux établissements de monnaie électronique exemptés en vertu des directives européennes pertinentes. Il ne s'appliquerait pas non plus aux petites institutions de retraite professionnelle. Ces entreprises et entités exemptées devraient néanmoins mettre en place un cadre de gestion des risques informatiques solide et documenté, lequel serait réexaminé au moins une fois par an.

Gouvernance et organisation

Les entités financières devront disposer d'un **cadre de gouvernance et de contrôle interne** qui garantisse une gestion efficace et prudente de tous les risques informatiques en vue d'atteindre un niveau élevé de résilience opérationnelle numérique. L'organe de direction devra mettre en place des procédures et des stratégies visant à garantir le maintien de normes élevées en matière de sécurité, de confidentialité et d' intégrité des données.

Identification, protection, prévention, détection des risques

Les entités financières devront entre autres i) examiner si nécessaire, et au moins une fois par an, la criticité ou l'importance des fonctions opérationnelles liées à l'informatique, ii) garantir que les données sont protégées contre les risques informatiques internes, y compris les risques liés à une mauvaise administration ou à un mauvais traitement et à une erreur humaine; iii) consigner tous les incidents liés à l' informatique ayant des effets sur la stabilité, la continuité ou la qualité des services financiers.

La **politique de continuité** des activités informatiques devrait avoir pour but de gérer et d'atténuer les risques susceptibles d'avoir une incidence préjudiciable sur les systèmes et les services informatiques des entités financières ainsi que de faciliter leur rétablissement rapide si nécessaire.

Les **programmes de sensibilisation** à la sécurité informatique devraient s'appliquer à l'ensemble du personnel, tandis que les formations à la résilience opérationnelle numérique devraient s'appliquer, au minimum, à tous les employés disposant de droits d'accès direct aux systèmes informatiques.

Notification des incidents majeurs liés à l'informatique

Les entités financières pourraient notifier, **sur une base volontaire**, les cybermenaces importantes à l' autorité compétente concernée lorsqu'elles estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients.

L'autorité compétente devrait être informée en tout état de cause **dans les 24 heures** suivant la prise de connaissance d'un incident en ce qui concerne les incidents qui perturbent de manière significative la disponibilité des services fournis par l'entité ou qui ont une incidence sur l'intégrité, la confidentialité ou la sécurité des données à caractère personnel conservées par l'entité financière. En ce qui concerne les incidents qui ont une incidence significative autre que la disponibilité des services fournis par l'entité financière, l'autorité compétente devrait être informée dans les 72 heures.

Dès réception du rapport d'incident, l'autorité compétente devrait fournir, dans les meilleurs délais, des précisions sur l'incident majeur lié à l'informatique à l'ABE, à l'AEMF ou à l'AEAPP, ainsi qu'à la BCE, le cas échéant. Le Conseil de résolution unique (CRU) devrait être informé lorsque l'entité financière touchée relève du règlement relatif au mécanisme de résolution unique, tandis que les centres de réponse aux incidents de sécurité informatique (CSIRT) devraient être avisés lorsque les entités touchées relèvent de la directive sur la sécurité des réseaux et des systèmes d'information (SRI).

Tests

Les tests de pénétration fondés sur la menace devraient couvrir au minimum **les fonctions et les services critiques ou importants** d'une entité financière. En outre, le texte a été modifié pour ce qui est de la participation des tiers prestataires de services informatiques aux tests de pénétration fondés sur la menace. Lorsque la participation d'un tiers prestataire de services informatiques est susceptible de porter atteinte à la qualité du service fourni à d'autres clients, ledit tiers prestataire aurait la possibilité de conclure des accords contractuels au nom de l'ensemble des utilisateurs de l'entité financière qui ont recours à ses services en vue de mener des tests groupés.

À l'issue du test, une fois que les rapports et les plans de mesures correctives ont été approuvés, l'entité financière et les testeurs externes devraient fournir à l'autorité publique unique désignée, conformément au règlement, un rapport confidentiel des résultats du test et la documentation confirmant que le test a été effectué conformément aux exigences.

Bonne gestion des risques liés aux tiers prestataires de services informatiques

Les entités financières devraient tenir et mettre à jour **un registre d'informations en rapport avec tous les accords contractuels** portant sur l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques qui appuient des fonctions critiques ou importantes. Les accords contractuels relatifs à l'utilisation de services informatiques devraient permettre aux entités financières de prendre les mesures correctives adéquates, qui pourront comporter **la résiliation complète des accords** si aucune rectification n'est possible ou la résiliation partielle des accords, dans certaines circonstances.

En vue de réduire les risques de perturbations au niveau de l'entité financière, dans des circonstances justifiées et en accord avec ses autorités compétentes, l'entité financière pourrait décider de ne pas résilier les accords contractuels conclus avec le tiers prestataire de services informatiques avant d'être en mesure de changer de tiers prestataire de services informatiques ou de recourir à des solutions sur site en fonction de la complexité du service fourni.

Enfin, lorsque des accords contractuels relatifs à l'utilisation de services informatiques qui appuient des fonctions critiques ou importantes sont conclus avec un **tiers prestataire de services informatiques établi dans un pays tiers**, les entités financières devraient également tenir compte du respect de la protection des données et de l'application effective des règles définies dans le présent règlement.