Gestion des risques : comprendre les obligations de votre entreprise dans le cadre du règlement DORA

Le règlement sur la résilience opérationnelle numérique[1] (Digital Operational Resilience Act – DORA) est entré en vigueur le 16 janvier 2023. DORA concerne tous les acteurs des services financiers de l'Union Européenne et leurs prestataires de services IT. Ces acteurs auront moins de 24 mois pour se conformer aux nouvelles exigences de la Commission Européenne en matière de cybersécurité, de gestion des risques IT et de résilience opérationnelle numérique.

Conçue pour renforcer la résilience numérique des entreprises du secteur des services financiers, DORA vise à normaliser et à renforcer un ensemble de réglementations nationales et de processus hétérogènes en matière de notification des incidents dans l'UE.[2] Le nouveau règlement loi devrait permettre de réduire les formalités administratives et les coûts élevés de mise en conformité.[3]

En harmonisant les règles et réglementations en matière de cybersécurité dans les 27 États membres de l'UE, l'objectif de DORA est d'aider les organisations à limiter les impacts des attaques cyber - en recrudescence - en imposant de nouvelles normes en matière de technologies numériques.[4] La nouvelle réglementation vise également à renforcer la stabilité et la confiance dans le secteur des services financiers de l'UE, à l'heure où de plus en plus de transactions financières s'effectuent en mode virtuel.[5]

L'évolution vers le numérique des transactions financières dans l'Union Européenne – tout comme les menaces et les attaques accompagnant l'augmentation des paiements en ligne - se produit à un rythme effréné. Une étude de la Commission Européenne montre qu'au début de la pandémie et en l'espace d'une semaine seulement, « l'utilisation des applications financières en Europe avait augmenté de 72 % ». [6] Dans le même temps, les cyberattaques contre les entreprises du secteur financier pendant la pandémie ont augmenté de 38 %, selon les données de la Commission.[7]

La gestion des risques numériques : l'un des 5 piliers de DORA

En élaborant DORA, les régulateurs européens ont défini deux piliers clés de gestion des risques : l'un couvrant la gestion des risques liés aux technologies numériques au sein des organisations (gestion des risques numériques), et l'autre la gestion des risques pour les prestataires IT et autres tiers délivrant des services numériques aux entreprises du secteur financier (gestion des risques numériques pour les tiers).

Si les deux piliers visent à intégrer les efforts de cybersécurité dans une stratégie plus large de gestion des risques d'une société financière, la gestion des risques numériques s'appuie sur la capacité d'une organisation à identifier, évaluer, contrôler et surveiller les risques liés à la résilience numérique, et à en rendre compte. Ce pilier fait également référence à la capacité d'une organisation à réagir et à rebondir suite à une attaque cyber ainsi qu'à mettre en œuvre les mécanismes nécessaires à la poursuite de ses activités, comme une gouvernance efficace, des responsabilités bien définies, ainsi que des stratégies efficaces de communication avec les différentes parties prenantes.

La gestion des risques numériques pour les tiers, quant à elle, désigne les processus mis en place par les organisations pour assurer la gestion efficace des risques liés aux tiers. Bien que variant pour chaque entreprise, cela peut inclure la capacité d'une organisation à créer des stratégies de sourcing et d'approvisionnement résilientes, à établir un registre des fournisseurs et à assurer des dispositions contractuelles solides en matière de cybersécurité.

5 questions à Thomas Hutin, Head of Cybersecurity France, sur la gestion des risques numériques qui sont au cœur des préoccupations des dirigeants.

Quelle est l'importance de la gestion des risques numériques pour les entreprises du secteur financier ?

Elle est critique. Dans le cadre du règlement DORA, les entreprises devront intégrer la gestion des risques numériques dans leurs stratégies d'entreprise. En outre, les dispositions relatives à la gestion des risques numériques devront s'inscrire dans un contexte métier, pour que les investissements soient correctement hiérarchisés et que les études d'impact soient menées en vue de renforcer la résilience des actifs les plus critiques. En conséquence, les dirigeants devront se montrer plus proactifs dans la compréhension de leurs risques numériques et dans leurs traitements. Plus que jamais, il est essentiel que les rôles et les responsabilités soient clairement définis de manière à fournir à la direction de l'entreprise les informations et les initiatives dont elle a besoin pour comprendre ces risques et y répondre.

Comment les entreprises du secteur financier peuvent-elles prioriser ces risques ?

Il faut commencer par évaluer ces risques numériques, les rendre visibles de la Direction et des différentes parties prenantes et mettre en place des processus de gouvernance et de surveillance efficaces. La surveillance des risques dans ce domaine doit être continue. Lorsqu'elles conçoivent leur approche, les entreprises du secteur financier doivent également tenir compte des risques de réputation ; le partage de l'information et le signalement des incidents doivent être inclus dans une stratégie de communication globale. Néanmoins et conformément à la législation sectorielle nationale et européenne, les entreprises du secteur financier peuvent confier les tâches de vérification du respect des exigences en matière de gestion des risques numériques à des entreprises intragroupe ou bien externes.

Ces efforts seront-ils ponctuels ou s'inscriront-ils dans une stratégie continue plus large ?

Une réponse courte serait : en permanence. Les stratégies de gestion des risques doivent être continuellement testées, afin de prouver leurs conformités et leurs efficacités. Les tests doivent intégrer des exercices axés sur le respect de la réglementation d'une part, et des campagnes de tests techniques (« TIBER » Threat Intelligence-based Ethical Red Teamin) joués par une « équipe adverse » qui reproduit les actions des attaquants afin d'évaluer les cyberdéfenses en temps réel. Il convient également de noter qu'une stratégie efficace de gestion des risques numériques dépend de la capacité à apporter des améliorations continues là où elles sont nécessaires. Le risque numérique ayant une nature dynamique, mieux vaut allouer des ressources à toute activité de remédiation.

Comment les entreprises du secteur financier peuvent-elles déterminer leurs risques liés aux tiers ?

La position de DORA sur la gestion des risques numériques par des tiers repose sur le principe suivant : si l'on peut externaliser un service, on ne peut pas externaliser un risque. Cela signifie que les entités impliquées restent entièrement responsables des risques qu'elles gèrent, indépendamment de la personne censée atténuer des risques spécifiques ou exploiter des services spécifiques. Il faut donc mettre davantage l'accent sur la diligence précontractuelle, qui doit garantir que les clauses de sécurité appropriées et la transparence en matière de risques soient pleinement intégrées au processus contractuel. En outre, les activités doivent disposer de processus d'évaluation des risques dédiés.

Que peuvent faire les entreprises de services financiers pour limiter leur exposition à ces risques ?

Le périmètre des services doit être soigneusement étudié et documenté. Les contrats doivent garantir que les services soient intégralement décrits, détaillant même les cas où le tiers pourrait lui-même sous-traiter des éléments du service. Compte tenu des nouvelles exigences en matière de reporting, il est aussi essentiel de veiller à ce que les obligations en matière de notification d'incidents et les délais associés soient documentés, et que les accords de niveau de service (ANS) soient plus généralement appropriés et bien définis.

Les 5 piliers de DORA

- la gestion des risques liés aux technologies de l'information et de la communication (TIC) ;
- la notification, aux autorités compétentes, des incidents majeurs liés à l'informatique ;
- les tests de résilience opérationnelle numérique ;
- le partage d'informations et de renseignements en rapport avec les cybermenaces et les cyber vulnérabilités ;
- les mesures destinées à garantir une gestion solide, par les entités financières, du risque lié aux tiers prestataires de services informatiques.

1: "Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014." European Commission. Sept. 24, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

2: Ibid.

3: Ibid.

4: "A Digital Finance Strategy for Europe – September 2020." European Commission. https://www.compete2020.gov.pt/admin/images/200924-digital-finance-factsheet_en.pdf

5: Ibid.

6: Ibid.

7: Ibid.

THOMAS HUTIN
Head of Cybersecurity
France