Committed to Europe

Position d'Orange sur la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité

Résumé

Orange soutient l'objectif de la proposition de Directive visant à établir des mesures pour assurer un niveau commun élevé de cybersécurité au sein de l'Union (SRI/NIS 2), qui abroge la directive NIS 1. Ce texte s'inscrit dans un cadre plus large d'instruments juridiques existants et d'initiatives futures visant à accroître la résilience des entités publiques et privées face aux cyber-menaces.

Une nouveauté importante est que le projet de directive SRI 2 met l'accent sur la gestion des risques au sein de la chaîne d'approvisionnement notamment en matière numérique. Toutefois il ne prévoit pas d'obligations pour les fournisseurs de solutions numériques, notamment les équipementiers ou fabricants de logiciels et de matériels numériques. Or, les chaînes d'approvisionnement sont de plus en plus globales et complexes, avec une multitude d'acteurs impliqués. De même, les réseaux de communications électroniques sont de plus en plus sophistiqués, tendance qui va s'accroître avec le passage à la 5G et à une infrastructure toujours plus virtualisée, reposant sur des logiciels (« software-based ») et des solutions de cloud. Pour garantir son efficacité, il est donc essentiel que le texte SRI 2 prévoit une allocation pertinente des responsabilités pour l'ensemble des acteurs de la chaine de valeur.

Orange considère que la proposition actuelle soulève un certain nombre de problèmes qui doivent être résolus au cours du processus législatif :

- Le projet SRI 2 vise à étendre son champ d'application à l'ensemble de la chaîne d'approvisionnement numérique, y compris les opérateurs de communications électroniques. Orange estime indispensable de responsabiliser au sein de cette chaine de valeur les principaux fournisseurs d'équipements numériques et de logiciels. Ces acteurs sont les mieux placés pour analyser et atténuer leurs propres vulnérabilités en matière de cybersécurité. Ils doivent être désignés comme entités essentielles.
- Le projet SRI 2 introduit une obligation de signaler les incidents «potentiels» dans un délai très court (24 heures), et prévoit des plafonds très élevés de sanctions en cas de non-respect. Orange considère que le signalement d'incidents «potentiels» (en plus des incidents significatifs) sera source d'incertitude juridique et de surcharge administrative. De plus, le délai de 24 heures pour les incidents significatifs est trop court et doit être allongé. Les plafonds de sanction en cas de non-respect sont excessifs et doivent être plus proportionnés.
- Le projet SRI 2 offre la possibilité aux entités établies dans plusieurs Etats membres de centraliser la gestion et le signalement des incidents dans l'État membre où elles ont leur principal établissement dans l'Union. Outre cette possibilité, Orange souhaite le maintien de la solution actuelle permettant d'avoir des établissements légaux dans plusieurs États membres afin de garantir la sécurité juridique et l'efficacité opérationnelle.
- L'inclusion des services de «centre de données» dans le champ d'application du projet SRI 2 repose sur une définition extensive qui crée une insécurité juridique. Cette définition doit ainsi être revue.

Avril 2021

La directive SRI 2 doit également s'appliquer aux principaux fournisseurs d'équipements numériques et de logiciels

L'article 18 de la directive SRI 2 prévoit que les entités essentielles et importantes, dont le secteur des communications électroniques, devront prendre les "mesures appropriées" pour évaluer et atténuer les risques pour la sécurité de l'ensemble des produits et services numériques sur lesquels elles s'appuient. Cette obligation n'est pas réalisable car les opérateurs télécoms ne maitrisent pas la conception des équipements numériques et logiciels ; ils n'ont accès ni au code ni à la conception des puces de l'ensemble des solutions numériques déployées dans leurs réseaux. Ils conçoivent et construisent leurs réseaux, et peuvent en revanche déterminer les solutions ou produits numériques sur lesquels s'appuient leurs applications critiques, afin d'identifier les technologies essentielles à leur fonctionnement. Les fournisseurs d'équipements et de logiciels qui conçoivent ces solutions ou produits sont les seuls acteurs en mesure d'analyser et d'atténuer leurs propres vulnérabilités en matière de cybersécurité.

Orange estime donc nécessaire de modifier substantiellement les articles 2 et 18 du projet SRI 2 en ce qui concerne la chaîne des responsabilités. Le champ d'application de SRI 2 doit être étendu aux fabricants d'équipements numériques et logiciels qui sont clefs pour les entités essentielles définies par le texte. Ainsi, les opérateurs de télécommunications devront identifier les technologies d'information, produits ou services sur lesquels s'appuient leurs applications critiques. Ces technologies, produits ou services identifiés seront alors considérés comme des entités essentielles.

L'article 21 permet aux États membres d'exiger que les entités essentielles et importantes certifient certains produits, services et processus numériques dans le cadre du Règlement Cybersecurité. La Commission est chargée d'adopter des actes délégués précisant quelles catégories d'entités essentielles sont tenues d'obtenir un certificat et quel type de certification. Or ces produits peuvent être soit développés par une entité essentielle ou importante, soit achetés à des tiers.

Si la certification des principaux produits/services/systèmes numériques est importante, Orange estime que la responsabilité de cette certification doit incomber aux équipementiers/fabricants de tels produits/services/systèmes. Enfin, la liste des produits numériques à certifier doit être établie conformément à l'article 18.1 (évaluation des risques).

Des améliorations à apporter aux dispositions en matière de signalement et de sanctions

Les obligations de signalement doivent mieux définir le champ d'application, le délai et les destinataires de la notification, en se limitant aux incidents significatifs et tangibles :

- Incidents potentiels : l'article 20 étend les obligations de signalement, en imposant la mise en place d'une procédure d'analyse des risques pour identifier et gérer les menaces potentielles. Cette mesure risque de submerger les autorités de notifications superflues, également facteur d'incertitudes. Les entités ne doivent avoir à signaler que les incidents significatifs et tangibles, et non les incidents «potentiels» : une telle obligation serait disproportionnée et irréaliste.
- Délai : le délai de 24 heures imparti aux entités importantes et essentielles pour effectuer leur notification initiale aux autorités compétentes ou au CSIRT est trop court : l'identification précise de l'incident et de sa cause peut prendre davantage de temps. Un délai de 72 heures serait plus raisonnable, et cohérent avec le délai prévu par le RGPD en cas de violation de la sécurité des données personnelles.

- Autorités compétentes : selon la proposition, les États membres pourront identifier les autorités compétentes ou le CSIRT pour la notification des incidents. Pour éviter la multiplication des notifications, chaque État membre devrait identifier un point unique pour le signalement.
- Sanctions : l'article 31.1 prévoit un niveau de sanctions très élevé. Le niveau des amendes doit être harmonisé et réduit. Cet article doit aussi s'appliquer aux principaux fournisseurs de technologies et de services numériques qui refusent de fournir des correctifs (« patches ») pour remédier aux incidents dans un délai raisonnable.

Maintenir la possibilité d'avoir des établissements légaux dans plusieurs Etats membres

En vertu de l'article 24, les fournisseurs de services DNS, les registres de noms de domaines de premier niveau, les fournisseurs de services d'informatique cloud, les fournisseurs de services de centres de données et de réseaux de diffusion de contenu, ainsi que certains fournisseurs de services numériques sont réputés relever de la juridiction de l'État membre dans lequel ils ont leur établissement principal dans l'Union. Orange ne s'oppose pas à cette disposition mais estime que la possibilité d'avoir des établissements légaux dans plusieurs Etats membres doit être maintenue pour les entités opérant sur plusieurs Etats mais n'ayant pas d'établissement principal.

Une approche plus équilibrée concernant les registres de vulnérabilités

Orange soutient les initiatives visant à coordonner la gestion des incidents de cybersécurité, mais s'interroge sur l'efficacité de répertorier et donner accès aux registres de vulnérabilités. Il est important de garantir la confidentialité et de clarifier le but et les bénéficiaires de l'accès.

En outre, toute divulgation et inscription au registre de vulnérabilités ne doit être effectuée que lorsque des mesures d'atténuation des risques sont possibles. Si celles-ci ne sont pas disponibles, un délai doit être imposé aux fournisseurs pour qu'ils adoptent des mesures d'atténuation de risque dans un délai raisonnable.

Enfin, la directive SRI 2 doit garantir que les modalités de communication actuellement en vigueur au niveau national entre l'autorité compétente et l'entité reste la voie privilégiée pour tout signalement.

Clarifier la définition de «service de centre de données»

La définition proposée de « service de centre de données » est si large que tout service reposant sur un centre de données entrerait dans le champ d'application de la directive SRI 2, quels que soient le nombre de clients concernés et le but du service fourni. Cette définition pourrait ainsi comprendre des services non critiques multi-accès de edge computing (par ex. des jeux vidéos), ce qui inquiète particulièrement le secteur numérique. La définition doit être clarifiée pour éviter toute insécurité juridique.

Garantir la cohérence des règles en matière de cybersécurité

La directive SRI 2 est proposée concomitamment à d'autres initiatives européennes en matière de cybersécurité, notamment la proposition de directive pour la résilience des entités critiques, le code des communications électroniques européen, la boîte à outils 5G, ou le projet de règlement «eIDAS ». Il est essentiel que le cadre législatif européen soit rationnel et clair pour l'ensemble des acteurs, afin d'éviter toute insécurité juridique et redondance des obligations.

Pour plus d'informations : https://www.orange.com/fr/groupe/orange-bruxelles, ou suivez-nous sur Twitter: @Orange_Brussels