DIGITALEUROPE

Transposition de la directive européenne sur la sécurité des réseaux et de l'information (RSI)

Bruxelles, le 5 Juillet 2016

EXECUTIVE SUMMARY

Le Conseil de l'Union européenne a publié la version définitive de la directive sur la sécurité des réseaux et de l'information (RSI) le 21 avril 2016. Alors qu'elle doit être officiellement signée par le Parlement européen cet été, le texte lui-même a déjà été accepté par les trois institutions européennes et ne devrait donc pas changer. Les États membres sont tenus de la transposer dans leur législation nationale dans un délai de 21 mois suivant son adoption. Afin de faciliter ce processus, veuillez trouver dans l'annexe ci-jointe un guide des meilleures pratiques sur la façon d'appliquer les aspects pertinents au secteur des technologies et entériner efficacement les intentions des rédacteurs.

La directive européenne RSI est le premier texte de loi sur la cybersécurité paneuropéen. Il se concentre sur le renforcement des autorités compétentes en matière de cybersécurité nationale, améliorant la coordination entre elles, et introduit des exigences de sécurité pour les acteurs sectoriels clés.

Aucune loi nationale ne devrait perdre de vue les deux objectifs principaux de la directive : (1) assurer un niveau élevé de cybersécurité pour les infrastructures critiques du pays ; (2) établir un mécanisme de coopération efficace entre les États membres de l'Union européenne afin de promouvoir cet objectif. Les ressources devraient d'abord et principalement être dédiées à la réalisation de ces deux objectifs essentiels.

En ce qui concerne le secteur des technologies, les dispositions liées aux dénommés fournisseurs de services numériques (FSN) sont d'un intérêt tout particulier. La directive indique clairement qu'il existe des différences fondamentales entre les opérateurs de services essentiels (OSE) et les FSN. En effet, ces derniers ne doivent pas être considérés comme des infrastructures critiques en tant que telles. Comme le reconnaît la loi, un incident touchant ces services numériques entraînerait un niveau considérablement moins élevé de risque pour la sécurité économique et la sécurité publique d'un pays. Maintenir cette distinction est donc essentiel afin de pouvoir également utiliser efficacement et effectivement les ressources limitées des autorités qui doivent superviser et imposer les règles.

Par conséquent, nous recommandons de porter une attention particulière à la portée envisagée des services en question et appelons les décideurs politiques à ne pas soumettre les secteurs, autres que ceux identifiés en tant que FSN et OSE, à des exigences de sécurité dans la législation nationale.

D'un point de vue de la juridiction, les FSN doivent pouvoir s'en remettre au droit en vigueur dans le pays de leur établissement principal, même lorsque les autorités compétentes de plus d'un pays sont impliquées. En ce qui concerne la surveillance, les autorités compétentes doivent suivre une approche ex post plutôt que d'imposer une obligation générale de supervision des FSN. En outre, elles doivent se concentrer sur les résultats et maintenir la distinction entreles OSE et les FSN en ne soumettant pas ces derniers à des exigences non prévues par la directive, telles que des instructions d'audit et mesures contraignantes.

DIGITALEUROPE
Rue de la Science, 14 – 1040 Bruxelles [Belgique]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Membre du registre de transparence de la Commission : 64270747023-20

Les mesures de sécurité s'appliquant aux FSN doivent être différentes de celles imposées aux OSE, puisque la directive énonce que ces derniers représentent un risque de sécurité considérablement moins élevé. Les décideurs politiques doivent réaliser l'objectif d'harmonisation de ces services, reconnaître les normes internationales du secteur existantes, éviter les mandats technologiques et respecter le droit des FSN entériné dans la directive afin de définir les mesures de sécurité les plus appropriées pour leurs systèmes. Les rapports d'incidents doivent également être harmonisés autant que possible au niveau européen. Ils doivent se concentrer sur les incidents affectant la continuité du service, respecter la flexibilité des délais de notification et créer un environnement de confiance encourageant l'échange d'information sans exposer la partie notifiante à une responsabilité accrue.

Les mesures imposées aux OSE affecteront également les autres industries, puisque les mesures de sécurité et les rapports d'incident se répercuteront dans les dispositions contractuelles, en particulier en ce qui concerne les services de cloud. Les FSN peuvent donc être indirectement sujets aux lois nationales de leurs clients et nous sommes par conséquent désireux de voir les mesures de sécurité reconnues sur la scène internationale s'appliquer à ces services. Nous proposons également une coordination et des synergies entre les exigences de rapport sur les OSE et les FSN, autant que possible, étant donné ces derniers peuvent être sujets à une double notification.

La directive définit l'ambition de parvenir à un niveau commun élevé de sécurité des réseaux et des systèmes d'information afin d'améliorer le fonctionnement du marché interne. Afin d'atteindre ce noble objectif , **les transpositions nationales doivent se concentrer sur une approche basée sur les risques, harmonisée et internationale harmonisée,** qui donne aux acteurs du secteur privé la flexibilité de s'adapter aux menaces en évolution constante, qui permette aux autorités de cybersécurité de concentrer les ressources limitées sur les défis les plus importants et qui reconnaîsse que la solution à un problème sans frontière doit être mondiale. Nous espérons que vous trouverez en ce guide un outil pratique à cette fin. Nous restons à votre disposition pour répondre à d'éventuelles questions.

Annexe : Guide des meilleures pratiques pour la mise en œuvre de la directive RSI

1. Fournisseurs de services numériques

a) Champ d'application

- La directive détermine que les marchés en ligne, les moteurs de recherche en ligne et les services informatiques hébergés doivent être considérés comme des fournisseurs de services numériques (FSN) et donc être inclus dans le champ de la directive. Alors qu'il s'agit d'une directive d'harmonisation minimale (article 2), il est important de maintenir une certaine cohérence au sein de l'Union européenne, et les États membres ne doivent donc pas soumettre les secteurs, autres que ceux identifiés en tant que FSN ou opérateurs de services essentiels (OSE), tels que défini dans l'article 3, à des exigences de sécurité dans la législation nationale.

- La directive indique explicitement que les fabricants de matériel informatique et les développeurs de logiciel ne sont pas des OSE ou FSN, et ne doivent donc pas être soumis aux lois nationales implémentant la directive (considérant 50).

- La directive exclut explicitement du champ d'application des marchés en ligne les services en ligne qui agissent en tant qu'intermédiaires par rapport aux services tiers lorsque la vente ou le contrat de service est finalement conclu (par ex. les sites de comparaison) (considérant 15).

- Les fonctions de recherche se limitant au contenu d'un site Internet spécifique ne doivent pas être considérées comme des moteurs de recherche en ligne, même si elles font appel à un fournisseur externe (considérant 16).

- La définition d'un service informatique hébergé en vertu de la directive dépend des ressources informatiques qui sont partagées par les multiples utilisateurs (article 4.19 et considérant 17). Les clouds privés (par opposition aux clouds publics) étant dédiés à une organisation unique, ils ne doivent pas être couverts.

- La directive souligne l'existence de différences fondamentales entre les OSE et les FSN, qui font que les FSN sont soumis à desrègles différentes (considérant 57). Une telle distinction doit être maintenue lors de l'implémentation de la directive.

b) Juridiction et surveillance

- La juridiction des FSN doit être attribuée à un seul État membre, au sein duquel se trouve l'établissement principal de l'opérateur dans l'UE, ce qui correspond en principe à l'endroit où se trouve son siège social au sein de l'UE (article 18.1 et considérant 64). Nous soutenons que les FSN doivent statuer eux-mêmes à cet égard et que cette décision doit uniquement être sujette à révision si les autorités compétentes la contestent dans le cadre d'activités de supervision ex post.

- Lorsque les FSN ont un réseau et des systèmes d'information dans des pays autres que celui de leur établissement principal, l'article 17.3 envisage la coopération des autorités compétentes. Cependant, du point de vue des FSN, il est important que le droit en vigueur reste celui du pays de leur établissement principal et qu'ils restent responsables uniquement vis-à-vis de l'autorité compétente de cette juridiction, qui agira en tant que leur interlocuteur.

- La directive souligne que les FSN sont sujets à une supervision ex post réactive et que les autorités compétentes n'ont donc pas d'obligation générale de superviser les FSN et ne doivent agir que si elles ont obtenu des preuves (article 17.1 et considérant 60). Ces dispositions doivent être respectées lors de l'implémentation de la directive.

- Dans le cas des FSN, les autorités peuvent uniquement demander des informations et exiger que les FSN remédient à tout problème, contrairement aux OSE. La directive pose clairement que les autorités n'ont pas de pouvoirs d'audit et qu'elles ne peuvent pas émettre d'instructions contraignantes. Ces dispositions doivent également être respectées au niveau national.

c) Exigences supplémentaires

- La sécurité et les exigences de notification des FSN sont sujettes à une harmonisation maximale (article 16.10). Cet article doit être considéré comme s'appliquant aux produits, services et solutions qui forment leurs réseaux et systèmes d'information. Par conséquent, des dispositions supplémentaires, telles que pour les tests de produits, ne doivent pas être requises dans la mesure où les produits et services sont utilisés dans ce contexte.

d) Mesures de sécurité et normes

- Les mesures de sécurité des FSN doivent être plus légères que celles des OSE. Les FSN doivent être libres de définir leur niveau de sécurité et de quelle façon ils souhaitent assurer la protection de leurs réseaux et systèmes d'information en fonction des risques présentés (considérant 49).

- Les mesures de sécurité doivent être orientées sur les processus et se concentrer sur la gestion des risques. Elles ne doivent pas exiger que les produits TIC soient conçus, développés ou fabriqués d'une façon particulière (considérant 51).

- La directive insiste sur le fait que les États membres ne doivent pas imposer d'autres exigences de sécurité aux FSN (article 16.10).

- Cependant, nous attendons des lignes directrices émanant de différents acteurs. Les États membres s'assureront que les mesures soulignées dans la directive sont adoptées (article 16.1), ils peuvent encourager l'utilisation de normes afin de les mettre en œuvre (article 19.1) et discutent des normes avec les organismes européens de normalisation du groupe de coopération (article 11.3 (h)). L'ENISA exprimera son opinion quant aux les normes appropriées (article 19.2) et la Commission européenne est chargée d'adopter des mesures d'exécution sur les mesures de sécurité (article 16.8).

- En raison de ce niveau de complication et des avantages de l'harmonisation, nous conseillons au processus national de s'en remettre fondamentalement aux mesures d'exécution pour l'acceptation des mesures appropriées, ce qui, dans tous les cas, doit être finalisé dans un délai d'un an après l'adoption de la directive. Les mesures d'exécution doivent être sans préjudice de la capacité des FSN à définir les mesures de sécurité, les plus appropriées pour leurs systèmes.

- L'article sur les normes permet aux normes européennes ou aux normes internationales d'être référencées (Article 19.1) En raison de la maturité des normes internationales appliquées dans ce domaine , nous recommandons que, lorsque des normes adéquates existent, une certification par rapport à l'une d'entre elles (telle qu'ISO 27001) soit suffisante pour satisfaire aux exigences.

- Quoi qu'il en soit, la certification des normes doit être optionnelle et non obligatoire. L'article 19 souligne que toute norme peut uniquement être « encouragée », et ce « sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un type particulier de technologies ».

e) Rapports sur les incidents de sécurité

- Comme pour les mesures de sécurité, plusieurs parties jouent un rôle dans la création des rapports d'incident en vertu de la directive RSI. Les États membres doivent s'assurer que les FSN notifient les incidents de sécurité qui ont un impact considérable sur la fourniture du service (qui est dans le champ d'application de la directive) qu'ils fournissent (article 16.3), le groupe de coopération est chargé de discuter des modalités de notification (article 11.3 (m)) et la Commission d'adopter les mesures d'exécution (articles 16.8 et 16.9).

- Une fois encore, nous recommandons que les transpositions nationales s'en remettent au processus des mesures d'exécution, dont celle concernant le seuil de notification et qui doit être adoptée dans un délai d'un an suivant la finalisation de la directive.

- En ce qui concerne les types d'incidents devant être signalés, les FSN sont chargés de notifier « tout incident ayant un impact significatif sur la fourniture de leur service » (article 16.3). À l'instar de la mise en œuvre des dispositions équivalentes pour les opérateurs de télécommunication, en vertu de l'article 13a de la directive-cadre sur les télécomunications, nous estimons que cela doit être interprété de manière à se concentrer sur **la continuité (ou la disponibilité)** des services fournis. En d'autres mots, les pannes qui atteignent un seuil particulier (à déterminer par le biais des mesures d'exécution) doivent être rapportés plutôt que tout autre type d'incident de sécurité. Cette approche présente l'avantage de se concentrer sur les incidents qui auront le plus probablement un impact sur l'économie ou la société, tout en minimisant (sans entièrement éliminer) un chevauchement avec les exigences de notification en cas de violation des données personnelles découlant du règlement général sur la protection des données.

- En outre, l'obligation de rapport pour les « opérateurs de services essentiels » stipule que ces opérateurs doivent notifier « les incidents ayant un impact significatif sur la continuité des services essentiels qu'ils fournissent », ce qui se concentre à nouveau clairement sur la continuité (ou la disponibilité) des services. Les co-législateurs sont d'accord pour dire que les obligations des FSN doivent être plus légères que celles des OSE (voir considérant 49). L'obligation de rapport des incidents pour les FSN en vertu de cette RSI ne doit donc pas être plus large que celle des OSE. En réalité, elle devrait même être davantage limitée en

termes de seuils. Cette situation souligne, à nouveau, que les rapports d'incidents pour les FSN doivent se limiter aux incidents qui atteignent un seuil spécifique et **affectent la continuité/disponibilité du service** et non les incidents liés à l'intégrité ou la confidentialité des données, qui sont en grande partie déjà couverts par les exigences de notification posées par le règlement général sur la protection des données et les règlementations eIDAS.

- En ce qui concerne le délai de notification, nous apprécions la flexibilité induite par le vocabulaire choisi dans le cas des rapports effectués « sans retard injustifié » (article 16.3). La mise en œuvre ne doit pas mener à des délais fixes, car les incidents varient considérablement du point de vue de leur complexité. L'uniformité des délais de rapport mèneraient à des rapports incorrects, où la portée initiale des systèmes concernés est vague et affecterait la capacité des professionnels d'intervention à prioriser une réponse aux incidents à la rédaction de rapport.

- Tel que mentionné, les incidents de sécurité devant être notifiés en vertu de la directive peuvent également l'être en vertu de la loi sur la protection des données , en fonction de si ces données personnelles ont été violées ou non. Cela n'implique donc pas seulement la rédaction d'un rapport pour un même incident à différentes autorités, mais ces autorités peuvent également être dans des États membres différents en fonction de la juridiction en vigueur pour le FSN en vertu des deux lois. Nous recommandons que les États membres reconnaissent la nécessité d'une notification unique des incidents, et visent à la prévoir, et cherchent à créer des canaux de communication afin de partager les informations pertinentes entre eux, sans porter préjudice à la confidentialité des activités.

- Les autorités compétentes doivent prendre en compte les conséquences commerciales et sur la réputation des FSN avant de partager publiquement des informations sur des incidents. Plus important encore : dévoiler l'incident pourrait accroître le risque en matière de sécurité. C'est pourquoi il est essentiel de s'organiser avec les acteurs concernés avant toute divulgation.

- La directive insiste sur le fait que les informations considérées comme confidentielles doivent être traitées en tant que telles (Considérants 41, 59, Article 1.5)

- L'article 16.3 souligne que la notification d'incidents de sécurité ne doit pas exposer la partie notifiante à une responsabilité accrue.

2. Opérateurs essentiels

a) Conséquences sur les mesures de sécurité

- Les FSN qui ont des OSE en tant que clients seront soumis aux mesures de sécurité en vigueur qui découlent des négociations contractuelles des obligations statutaires pour les opérateurs essentiels (article 14.1). Ainsi, ils peuvent être directement soumis au droit national de leurs clients, indépendamment du droit applicable dans le pays de leur siège principal européen.

- Par conséquent, des efforts d'harmonisation des mesures de sécurité pour les opérateurs essentiels seraient les bienvenues. Alors que les États membres ont le droit d'imposer des obligations plus strictes sur les opérateurs essentiels que celles définies dans la directive (article 3), nous recommandons une

certaine retenue en la matière et nous encourageons les États membres à travailler à la mise en place d'une approche harmonisée. Il est possible d'y parvenir en évitant des mesures supplémentaires dans les transpositions nationales et en cherchant à déterminer des mesures de sécurité adéquates dans le groupe de coopération plutôt que de se concentrer sur le processus national.

- Les exigences de sécurité doivent se fonder autant que possible sur les normes internationales (telles que les séries ISO 27x) et être reconnues en tant que meilleures pratiques de sécurité.

- Les mesures de sécurité imposées sur les OSE ne doivent en aucun cas exiger que des produits TIC spécifiques soient conçus, développés ou fabriqués d'une façon particulière (considérant 51).

b) Conséquences sur les rapports d'incidents de sécurité

- Les opérateurs de services essentiels sont tenus de rapporter les incidents de sécurité aux FSN avec qui ils ont conclu un contrat etqui affectent la continuité de leurs services essentiels (article 16.5). Les FSN devront donc, en vertu du contrat, faire rapport à l'opérateur essentiel en question des incidents de sécurité qui peuvent le toucher.

- Nous apprécions la flexibilité au niveau du délai de notification pour les OSE inhérents à la phrase « sans retard injustifié » (article 14.3). Les transpositions nationales ne doivent pas introduire de délais spécifiques et, dans tous les cas, s'il est demandé aux OSE de justifier le délai de notification, la durée par rapport à laquelle ils sont évalués doit commencer lorsque l'OSE a été averti de l'incident, et non au moment auquel le FSN en a été averti.

- L'article 14.7 envisage l'élaboration de lignes directrices relatives aux circonstances de notification par le groupe de coopération par opposition au rôle d'harmonisation de la Commission pour les notifications des FSN. En raison des exigences de double rapport pour les FSN, il est important que les exigences de notification respectives ne soient pas contradictoires et soient alignées autant que possible. Ce processus doit donc être approuvé par rapport à cet objectif. En outre, les exigences de notification des FSN doivent respecter les obligations de confidentialité qu'ils ont à l'encontre de leurs clients OSE et ne pas leur demander de partager des informations confidentielles professionnelles.

À PROPOS DE DIGITALEUROPE

DIGITALEUROPE est la voix de l'économie numérique européenne. Nos membres comprennent certaines des plus grandes sociétés informatiques, de technologies de l'information et des communications, et des associations nationales de toute l'Europe. DIGITALEUROPE souhaite que les entreprises et citoyens européens bénéficient totalement des technologies numériques et que l'Europe augmente le nombre, attire et retienne les meilleures entreprises de technologie numérique au monde.

DIGITALEUROPE assure la participation du secteur au développement et à la mise en œuvre des politiques européennes. Les membres de DIGITALEUROPE incluent 62 entreprises et 37 associations professionnelles nationales de toute l'Europe. Notre site Internet fournit davantage d'informations sur nos dernières nouvelles et activités : http://www.digitaleurope.org

MEMBRES DIGITALEUROPE

ENTREPRISES

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Associations professionnelles nationales

Allemagne : BITKOM, ZVEI
Autriche : IOÖ
Belgique : AGORIA
Biélorussie : INFOPARK
Bulgarie : BAIT
Chypre : CITEA
Danemark : DI Digital, IT-BRANCHEN
Espagne : AMETIC
Estonie : ITL
Finlande : FFTI
France : AFNUM, Force Numérique, Tech in France
Grèce : SEPE
Hongrie : IVSZ
Irlande : ICT IRELAND
Italie : ANITEC
Lituanie : INFOBALT
Pays-Bas : Nederland ICT, FIAR
Pologne : KIGEIT, PIIT, ZIPSEE
Portugal : AGEFE
Roumanie : ANIS, APDETIC
Royaume-Uni : techUK
Slovaquie : ITAS
Slovénie : GZS
Suède : Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Suisse : SWICO
Turquie : Digital Turkey Platform, ECID
Ukraine : IT UKRAINE