FEDIL

Member News

DIRECTIVE NIS : QUELLES EXIGENCES POUR LES FOURNISSEURS DE SERVICES NUMÉRIQUES AU LUXEMBOURG ?

La transposition de la directive européenne 2016/1148 dite « Directive NIS » impose de nouvelles exigences réglementaires à un ensemble d'acteurs dont les systèmes informatiques soutiennent des fonctions sociétales fondamentales. Les entreprises désignées comme étant Opérateurs de Services Essentiels ainsi que les Fournisseurs de Services Numériques, dont notamment les acteurs du Cloud au Luxembourg, sont concernés par cette nouvelle législation. Afin de mieux comprendre les tenants et aboutissants pour chacun de ses membres, Cloud Community Europe Luxembourg, l'association des sociétés actives dans le Cloud Computing, est allée à la rencontre de Luc Tapella, Directeur de l'ILR, l'Institut Luxembourgeois de Régulation. A noter que la FEDIL, Cloud Community Europe et Finance & Technology Luxembourg proposent en collaboration une séance d'information à destination des Fournisseurs de Services Numériques le lundi 3 février 2020 dans les locaux de la FEDIL.

De gauche à droite: Michèle Bram (directrice adjointe), Luc Tapella (directeur) et Camille Hierzig (directeur adjoint) – Photo (c) ILR/Luc

Monsieur Tapella, pouvez-vous nous préciser quels sont les objectifs visés par la directive NIS ?

Luc Tapella : Au cœur de nos sociétés, le numérique occupe une dimension primordiale. De nombreux services dépendent de la disponibilité des données et des réseaux, et certains sont essentiels pour tout un chacun. Parmi eux, notons certaines fonctions financières, d'autres dans le domaine de la santé ou encore l'approvisionnement en énergie. La numérisation de la société s'accompagne d'une exposition croissante au risque cyber. À travers la directive NIS, la Commission européenne entend assurer un niveau élevé de sécurité des réseaux et des systèmes d'information, harmonisé à l'échelle de l'Union européenne. À ce titre, la directive NIS et ses transpositions en lois nationales par les Etats Membres visent les opérateurs fournissant des services essentiels. Cette démarche s'inscrit aussi dans le développement d'un marché digital unique, en garantissant l'application du même niveau de normes dans l'ensemble des pays membres. La NIS renforce la sécurité, donc aussi la résilience des systèmes permettant la fourniture des services les plus omniprésents dans nos vies. Elle prévoit la mise en œuvre des mesures qui permettent d'assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union européenne (UE).

Cette directive a dû être transposée dans le droit de chaque pays membre de l'UE. Que peut-on dire de sa mise en œuvre au niveau du Luxembourg ?

Luc Tapella : Le Luxembourg l'a transposée sans pratiquement rien changer à son contenu. Nous appliquons les normes édictées aux secteurs spécifiquement visés par la directive : l'énergie, le transport, les banques et infrastructures de marchés financiers, la santé, l'eau et les infrastructures numériques. D'autres pays ont étendu la liste des secteurs visés, comme la France par exemple, qui y a inclus les acteurs de la chaîne agroalimentaire. Il est important de noter que chaque pays a défini des autorités compétentes en la matière. Au Luxembourg, on en compte seulement deux : la CSSF pour les acteurs du secteur financier, et l'ILR pour l'ensemble des autres acteurs.

La directive et sa transposition dans le droit luxembourgeois distinguent deux catégories d'acteurs, à savoir les Opérateurs de Services Essentiels et les Fournisseurs de Services Numériques. Comment la législation s'applique-t-elle à chacun d'eux ?

Luc Tapella : Les Opérateurs de Services Essentiels (OSE) sont donc les acteurs gérant des activités dans les domaines de l'énergie, des transports aérien, ferroviaire, routier ou même encore fluvial ou maritime, de la finance, à savoir les banques et les infrastructures de marchés financiers, de la santé avec les établissements de soins, et de la fourniture et distribution d'eau potable. Il s'agit d'opérateurs dont la compromission des systèmes informatiques ou des réseaux pourrait avoir des conséquences critiques sur les services qu'ils fournissent. Nous sommes actuellement occupés à définir lesquels, parmi les acteurs actifs dans ces domaines, relèveront des OSE. Il faut savoir qu'aucune liste relative à ces acteurs ne sera publiée. Autrement dit, les opérateurs qui n'auront pas été contactés et désignés comme tels par le régulateur ne devront pas répondre aux exigences définies dans la loi.

Pour ce qui est des Fournisseurs de Services Numériques (FSN), on distingue trois catégories d'acteurs : les places de marché en ligne, les moteurs de recherche en ligne et les services informatiques dans le Cloud. Parmi ces acteurs, tomberont sous la législation ceux ayant leur établissement principal au Grand-Duché de Luxembourg ou ayant désigné leur représentant dans l'Union européenne au Grand-Duché de Luxembourg, employant plus de cinquante personnes ou ayant un chiffre d'affaires supérieur à dix millions d'euros.

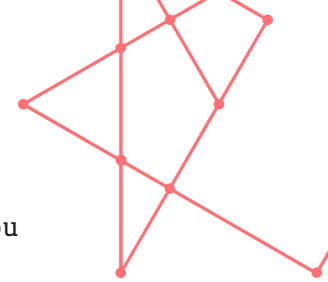
Quelles sont les nouvelles obligations pour les Fournisseurs de Services Numériques concernés ?

Luc Tapella : Pour ces acteurs, la régulation est moins lourde que pour les OSE dans la mesure où ils ne seront pas soumis à un reporting régulier. Néanmoins, la loi requiert de la part des FSN d'identifier « les risques qui menacent la sécurité des réseaux et des systèmes d'information » qu'ils utilisent pour offrir leurs services dans l'Union, et qu'ils prennent « les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer ». Les Fournisseurs de Services Numériques doivent en outre signaler à leurs clients OSE tout incident ayant un impact significatif sur la continuité des services essentiels. Ils doivent également notifier les autorités compétentes, conformément aux exigences du Règlement d'exécution européen 2018/151 précisant les éléments à prendre en considération par les fournisseurs de services numériques pour gérer les risques ainsi que les paramètres permettant de déterminer si un incident a un impact significatif. En d'autres termes, ces acteurs, comme ils y étaient pour la plupart déjà obligés, doivent mettre en place des éléments de sécurité adaptés, avoir une politique de gestion des incidents ainsi que de gestion de la continuité des activités, assurer un suivi avec des audits et contrôles et documenter l'ensemble. La loi luxembourgeoise transposant la directive NIS introduit simplement pour eux une obligation de notification à l'ILR en cas d'incident.

Quand les Fournisseurs de Services Numériques doivent-ils notifier les incidents ?

Luc Tapella : Quand un des cas de figure défini par le règlement d'exécution de l'UE (2018/151) entre en ligne de compte :

- le service a été indisponible pendant plus de 5.000.000 heures-utilisateur ;
- l'incident a entraîné une perte d'intégrité, d'authenticité ou de



confidentialité ayant touché plus de 100.000 utilisateurs dans l'UE ;
- l'incident a engendré un risque pour la sécurité ou la sûreté publique, ou un risque pouvant entrainer un décès ;
- l'incident a causé un préjudice matériel à au moins un utilisateur dans l'Union dès lors que le préjudice causé à cet utilisateur dépasse 1.000.000 euros.

Au regard de ces critères et de la taille du marché luxembourgeois, nous ne nous attendons pas à recevoir beaucoup de notifications, sauf pour certains FSN globaux ou européens, étant donné que ces seuils concernent tout le marché du FSN au sein de l'UE. Toutefois, les acteurs doivent avoir conscience de ces obligations.

Au Luxembourg, les Fournisseurs de Services Numériques que sont les PSF de support tombent sous la régulation de la CSSF. À quel régulateur doivent-ils rendre des comptes ?

Luc Tapella : Parce qu'ils gèrent des données financières ou des infrastructures informatiques d'acteurs financiers entre autres, ces acteurs doivent potentiellement répondre à deux autorités. Nous sommes actuellement en discussion avec la CSSF afin de pouvoir préciser à ces acteurs leurs obligations. D'autre part, nous travaillons à la mise en œuvre d'une plateforme unique de notification, qui doit permettre à chaque acteur de ne pas avoir à multiplier les démarches vis-à-vis de l'ensemble des autorités compétentes.

Face à quels éléments les Fournisseurs de Services Numériques doivent-ils être vigilants ?

Luc Tapella : Tout en ne tombant pas dans les critères les obligeant à notifier un incident, des acteurs proposant des services Cloud, qu'il s'agisse d'infrastructure informatique, de plateforme ou de software, peuvent très bien être sous-traitants d'un Opérateur de Services Essentiels. Parce que ce dernier est tenu de nous signaler divers incidents ou de rapporter diverses informations, certains éléments contractuels pourraient être adaptés afin de répondre aux exigences. En cas d'incident signalé par l'OSE, nous pourrions aussi exiger du Cloud Provider qu'il nous livre une série d'informations. Il faut aussi que chacun ait conscience que la liste des OSE est amenée à évoluer avec le temps en fonction des évolutions du marché ou encore de la technologie mise en œuvre.

Enfin, je voudrais attirer l'attention sur le fait que les OSE, même si les seuils édictés par la loi ne sont pas atteints, ont toujours la possibilité de procéder à des notifications volontaires. Ces notifications volontaires doivent nous permettre de mieux comprendre les mécanismes à l'œuvre et à davantage contribuer, en tant que point de contact national unique en matière de sécurité des réseaux et des systèmes d'information (SPOC), à la dynamique poursuivie par la NIS à l'échelle européenne.

***Pour en savoir plus, une** séance d'information **à destination des** Fournisseurs de Services Numériques est organisée à la FEDIL le lundi 3 février 2020 à 16h00.*

Infos ? www.fedil.lu/fr/events

Cloud Community Europe Luxembourg : la directive « NIS » essentielle à la construction d'un marché digital unique.

« Pour Cloud Community Europe Luxembourg, l'association représentant les acteurs du Cloud Computing, affiliée à l'organisation ICTluxembourg ainsi qu'à la FEDIL, la directive NIS s'inscrit au cœur même d'une immense opportunité mais aussi d'un défi primordial pour nos sociétés : la construction du « Digital Single Market » européen.

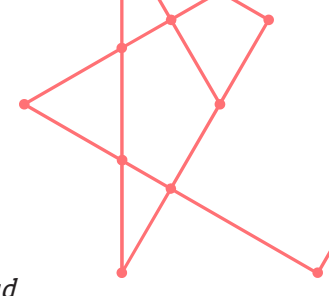
L'espace européen unique garantit à ce jour quatre libertés : la libre circulation des personnes, des capitaux, des services et des biens. Une cinquième liberté se met enfin en place : la libre circulation des données. En mai 2018, le RGPD a donné un cadre puissant à la protection des données personnelles. En complément, le règlement sur le libre flux des données non-personnelles applicable depuis mai 2019 a ouvert un véritable espace pour exploiter au mieux et de manière sécurisée le potentiel des technologies digitales. Par ailleurs, le CyberSecurity Act de l'EU, en vigueur depuis juin 2019, confirme l'importance de gérer les risques cyber à l'échelle européenne.

Enfin, la régulation NIS constitue une pièce maîtresse dans la construction d'une Europe digitale forte et de confiance, une Europe cyber-résiliente. Elle vise à protéger les services essentiels ainsi qu'à renforcer les Opérateurs de Services Essentiels (OSE) et les Fournisseurs de Services Numériques (FSN), tels que les « Cloud Providers ». Pour les acteurs luxembourgeois du Cloud Computing, la construction du « Digital Single Market » est vitale. Dans ce cadre, la directive NIS constitue une réelle opportunité pour assurer un écosystème digital encore plus résilient face aux menaces croissantes, mais également pour attirer de nouveaux acteurs de l'international vers le Luxembourg et pour promouvoir notre savoir-faire dans le nouvel espace digital européen. »

Yves Reding – Président de Cloud Community Europe – Luxembourg

About Cloud Community Europe Luxembourg

Cloud Community Europe Luxembourg (formerly "EuroCloud Luxembourg") was founded in December 2009 with the support of Fedil – Business Federation and the ABBL, in an impulse to position Luxembourg on the European map for Cloud Computing and SAAS, and encourage the adoption of such technologies at national level.



Its missions are numerous and can be outlined as follows:

– Contribute to the development of the cloud computing business in Luxembourg by creating an exchange platform, a « Cloud ecosystem » for cloud service providers;

– Promote and encourage the uptake of cloud services and applications on a national and international level;

– Participate in the development of a legal framework for cloud computing on a national and European level;

– Support cloud computing companies thanks to the presence of major cloud experts, as well as best practices sharing and a strong coordination with Cloud Community Europe associations throughout Europe.

Cloud Community Europe – Luxembourg is an association made in Luxembourg and created by key and enthusiastic experts from the ICT industry, all striving to enhance competitiveness and innovation. The association is also part of the larger pan-European network, Cloud Community Europe.