Consultation européenne sur la Directive NIS 2
Contribution de Syntec Numérique et TECH IN France

L'accélération de la transformation numérique dans les entreprises a entrainé la mise en place de nouveaux systèmes d'information ou de nouvelles briques sur les systèmes existants, ce qui a conduit à un accroissement des potentiels vulnérabilités et d'une plus grande surface d'exposition aux cyber attaques provenant d'acteurs malveillants de tout type (Etats, cybercriminels, hackeurs, etc.). De plus, la crise sanitaire a eu des conséquences sur la gestion de la sécurité informatique des entreprises, avec une augmentation du recours au télétravail dans les entreprises, et ce, sans que les salariés ne soient systématiquement formés aux enjeux de la cybersécurité.

Le secteur numérique tient à rappeler l'enjeu fondamental que constitue la sécurité des réseaux et systèmes d'information pour les entreprises. La directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS) a permis d'améliorer et d'harmoniser la préparation de l'Europe à la cybersécurité aux niveaux national et européen. Elle est un élément clé pour rendre l'Europe plus résiliente et assurer une réponse aux cyber menaces actuelles.

Syntec Numérique et TECH IN France se félicitent que la Commission européenne se saisisse du sujet afin de renforcer l'harmonisation de la cybersécurité des États membres tout en prévoyant des mesures qui prennent en considération les défis les plus récents auxquels l'Europe est confrontée en matière de cybersécurité.

Nous souhaitons, à cet égard, porter à votre attention nos principales recommandations sur le sujet.

Champ d'application

Il est essentiel que l'Europe protège et mette en place des mesures qui, à terme, amélioreront la résilience des entreprises et des Etats membres en matière de cybersécurité. Il s'agit là de l'objectif de la proposition de directive NIS 2, qui exige non seulement l'adoption de stratégies nationales de cybersécurité (réexaminées tous les deux ans), mais aussi que les États membres déterminent quelles sont les entités jugées essentielles pour leur économie et la société.

- Le champ d'application initiale de la Directive NIS avait permis de faire la distinction entre opérateurs de services essentiels (OSE) et fournisseurs de services numériques (FSN). Avec la progression constante de la transformation numérique, la Commission européenne a constaté que cette distinction n'était plus adaptée et que d'autres entités pouvaient être considérées comme essentielles ou importantes.

- La proposition de la Commission marque une extension du champ existant de la directive NIS. A ce jour, l'analyse des risques afférents à l'ajout de nouveaux secteurs vulnérables aux cyberattaques est un élément manquant du texte.

- Il convient de privilégier une approche proportionnée en justifiant l'ajout de ces nouveaux secteurs à la proposition. Il apparaît nécessaire de préciser que l'ajout du *manufacturing* dans la catégorie des OSE (notamment pour la santé) et des opérateurs importants est limitée aux

usines dont la production est localisée dans l'Union Européenne. Cet amendement pourrait remettre en question les pratiques établies de sécurisation des chaînes de valeur.

Champ d'application pour les PME et micro-entreprises

Autre changement, la proposition de directive NIS 2 indique explicitement que les entreprises définies comme « micro- entreprises et entreprises de petites tailles » devraient rester hors du champ d'application de la directive.

- Nous partageons cette approche : l'ajout de restrictions et d'obligations de conformité complexes aux plus petites entreprises empêcherait leur croissance.

- En outre, la plupart des PME ne seraient pas considérées comme essentielles ou suffisamment importantes pour entrer dans le champ d'application de la directive NIS (Considérant 8).

- Toutefois, l'approche adoptée par la proposition entraînera probablement une plus grande fragmentation dans les États membres. La proposition indique que les États membres pourraient également produire un critère de définition visant à déterminer quelles PME seraient considérées comme essentielles ou importantes pour l'État membre en question (Considérant 9). Ceci pourrait provoquer une fragmentation accrue et un manque de clarté pour les PME qui opèrent dans plusieurs États membres : elles pourront relever du champ d'application d'un État membre mais pas d'un autre.

- La garantie que les PME non essentielles restent en dehors du champ d'application n'est pas claire. L'investissement dans la réalisation d'une meilleure résilience technologique en matière de cybersécurité doit être l'objectif principal. L'écart de cyber-résilience entre les grandes et les petites entreprises doit être comblé, notamment si le champ d'application est élargi. C'est notamment le cas pour les petites entreprises qui manquent de compréhension, d'investissements et de ressources pour contrer les cyber-attaques.

La Directive indique toutefois que, quelle que soit leur taille, elle s'applique également aux entités visées aux annexes I et II, dans les cas suivants :

- Les services sont fournis par l'une des entités suivantes :
  - Réseaux de communications électroniques publics ou des services de communications électroniques accessibles au public (annexe I) ;
  - Prestataires de services de confiance (annexe I) ;
  - Registres des noms de domaines de premier niveau ;
  - Prestataires de services du système de noms de domaines (annexe I).

- L'entité est une entité d'administration publique (Article 4),
- L'entité est le seul prestataire de services dans un État membre ;
- L'entité est critique en raison de son importance au niveau régional ou national pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre ;
- L'entité est identifiée comme une entité critique conformément à la future directive sur la résilience des entités critiques

Opérateurs de services essentiels (OSE)

L'une des principales évolutions avancées par la proposition de directive NIS porte sur l'élargissement des entités définies comme « opérateurs de service essentiel » (OSE). La liste des OSE comprend maintenant des entités du secteur de la santé (fabricants de dispositifs médicaux), des installations de R&D, des fournisseurs de cloud, etc.

- La proposition prévoit que la liste des OSE inclut une « section d'infrastructure numérique » qui comprend : fournisseurs de points d'échange internet ; fournisseurs de services DNS ; registres de noms de domaines de premier niveau ; fournisseurs de cloud ; datacenters ; fournisseurs de réseaux de diffusion de contenu ; prestataires de services de confiance ; fournisseurs de réseaux de communications électroniques publics).

- Sur la partie santé, il semble nécessaire d'avoir une définition claire et une description concise de ce qu'est un fabricant de dispositifs médicaux.

- Les FSN qui fournissent des services dans plusieurs États membres, relèveront de la juridiction de l'État membre dans lequel ils ont leur principal établissement. Cette mesure permettra d'éviter tout chevauchement réglementaire.

- En élargissant le champ d'application et le nombre de prestataires de services classés comme OSE, la proposition ne tient pas compte, dans sa formulation actuelle, des cas de figure où un OSE fournit des solutions d'hébergement à un autre OSE. Il convient de se demander si les obligations contractuelles des fournisseurs de services seront reconnues dans ces circonstances. Ceci pourrait entraîner une ambiguïté juridique et/ou un chevauchement des obligations de notification, les fournisseurs de solutions d'hébergement devant signaler au régulateur un incident affectant leurs clients.

Entités importantes

Les entités officiellement considérées comme des « fournisseurs de services numériques » (FSN) dans la directive NIS sont à présent indiqués comme « entités importantes » dans la nouvelle proposition. Ces entités importantes seront réglementées ex post.

La liste des entités importantes a été élargie et comprend : les services postaux et de courrier, la gestion des déchets, la production alimentaire, l'industrie manufacturière, les market places, les moteurs de recherche en ligne et les réseaux sociaux. Comme ces entités ne sont pas définies comme essentielles ou critiques, elles seront réglementées *ex post*.

- Dans la section « manufacturing », toute organisation qui est un fabricant d'équipements électriques, informatiques, électroniques, optiques, de machines, de véhicules et de transports est concernée. Cette disposition s'appliquera à presque toutes les entreprises manufacturières en Europe. Une description plus détaillée des types d'entités qui devraient être considérées comme importantes est nécessaire.

Encourager l'harmonisation et la coopération réglementaire

Harmonisation entre les Etats membres

L'un des principaux objectifs de la proposition de directive NIS 2 est d'améliorer l'harmonisation entre les États membres et de réduire la fragmentation. Avec la directive NIS, les États membres ont été invités à mettre à jour la liste des OSE pour y inclure les entités jugées essentielles à l'économie de l'État membre concerné. Cela a entraîné une fragmentation importante dans toute l'Europe.

- La proposition de la Commission marque une avancée significative en matière d'harmonisation réglementaire, en particulier en ce qui concerne les obligations de déclaration et les exigences en matière de gestion des risques dans différentes lois. Nous saluons ainsi l'ambition d'harmoniser la proposition NIS 2 avec les autres législations applicables à la cybersécurité identifiées dans l'article 2. Il reste toutefois essentiel d'éviter les lacunes sectorielles, en s'assurant que le niveau d'exigence de base (prévu par NIS 2) s'applique de manière identique dans tous les secteurs dans lesquels les entités opèrent. Il conviendrait pour cela de modifier des dispositions de l'article 2(6) afin d'éviter les chevauchements réglementaires (notamment en termes de mesures de gestion des risques cyber ou d'exigences en matière de rapports) et assurer un alignement des dispositions sectorielles de la proposition avec les dispositions pertinentes de la présente directive.

- Le fait que la Commission maintienne le texte sous la forme d'une directive et non d'un règlement, permet une certaine flexibilité lors de la transposition. Toutefois, elle propose de supprimer l'obligation pour les États membres de produire une liste nationale des OSE et, pour la remplacer, de proposer une liste européenne des OSE.

- L'harmonisation entre États membres devrait aller encore plus loin, notamment en ce qui concerne l'identification des autorités compétentes des États membres qui superviseront l'application des entités couvertes par NIS 2. La proposition prévoit que les États membres identifient et désignent au moins une autorité compétente de surveillance (ils auront la possibilité de désigner plus d'une autorité compétente).

- En outre, les nouvelles mesures punitives qui seront mises à la disposition des États membres pourraient également présenter des disparités en termes de niveau d'application cohérente. À cet égard, nous recommandons aux États membres de transposer leur législation nationale aussi près que possible de la proposition NIS 2 et à la Commission de publier des lignes directrices détaillées pour contribuer à l'harmonisation.

Coopération entre les Etats membres et les entreprises

La directive créée un cadre pour la divulgation coordonnée des vulnérabilités et impose aux États membres de désigner des CSIRT qui agiront en tant qu'intermédiaires de confiance et faciliteront les interactions entre les entités effectuant le signalement et les fabricants ou les fournisseurs. L'ENISA sera tenue de produire et de tenir à jour un registre européen des vulnérabilités recensant les vulnérabilités constatées.

- En matière de coopération, il pourrait être intéressant de proposer un cadre dans lequel l'autorité nationale compétente (comme le CSIRT) joue le rôle de facilitateur entre chercheurs et fabricants (industrie) dans la divulgation de la vulnérabilité. Ceci constitue une réelle valeur ajoutée pour la coopération public/privée. Nous accueillons favorablement la possibilité d'impliquer l'industrie dans le réseau CSIRT et le groupe de coopération NIS. Il conviendrait

d’apporter des précisions sur la relation public/privé, notamment en termes d’engagement concret.

- Il pourrait être intéressant de mieux préciser les objectifs des registres centralisées au moment de fournir ce mandat à l’ENISA.

Les États membres, avec le soutien de l'ENISA, ont récemment lancé le réseau CyCLONe, qui vise à faciliter la coopération en cas de cyberincidents. CyCLONe veille à ce que les informations circulent plus efficacement entre les différentes structures de cybersécurité des États membres et permettra de mieux coordonner les stratégies de réponse nationales et les évaluations d'impact.

- Les véhicules de coopération comme CyCLONe pourraient bénéficier de la participation de l'industrie, dont les représentants peuvent apporter une vision de l’environnement des menaces. L'implication et le développement proactif de canaux de communication avant un incident peuvent améliorer considérablement l'environnement de cybersécurité. Il serait intéressant d’ouvrir aux OSE la participation aux activités de CyCLONe, permettant de renforcer la coopération entre le secteur privé et le secteur public en la matière.

Garantir une cohérence réglementaire

Avec la nouvelle proposition d'élargissement du champ d'application de la NIS et les propositions législatives supplémentaires qui sont examinées simultanément, il est maintenant plus important que jamais de garantir un niveau élevé de cohérence entre toutes les autres législations.

- Avec l'élargissement de la portée de la liste des OSE pour inclure les fournisseurs de réseaux de communications électroniques, NIS 2 doit prendre en considération le Code européen des communications électroniques (EECC). Parallèlement, la Commission propose un règlement sur la résilience numérique du secteur financier (Règlement DORA).

- Il convient de tenir compte des exigences de déclarations relatives au RGPD : si une OSE ou une entité importante est confrontée à un incident qui implique la violation de données à caractère personnel, elle est tenue de signaler le même incident à deux autorités distinctes.

- La crise du Covid-19 et les récentes cyberattaques suscitent un regain d'attention pour la protection de certains secteurs et infrastructures critiques. Dans la mesure où de nouvelles réglementations sectorielles pourraient voir le jour, il est nécessaire de veiller à un alignement entre les dispositions juridiques horizontales et sectorielles pour éviter un chevauchement.

- La Commission propose la création d’un registre commun des OSE. Nous pensons que la création d’un tel registre au niveau européen créerait une charge administrative supplémentaire, dans la mesure où plusieurs Etats membres contiennent déjà cette disposition.

- Enfin, une cohérence entre les diverses dispositions législatives en cours d’élaboration ou de révision est clé, dans la mesure où les entités critiques seront soumises simultanément à plusieurs initiatives (directive NIS 2, directive sur la résilience des entités critiques, et futurs systèmes de certification cybersécurité).

Obligations des entités

Avec la nouvelle proposition NIS 2, s'ajoutent de nouvelles obligations pour les OSE et les entités importantes.

Obligations s'appliquant aux OSE

- Nous saluons la démarche de la Commission visant à rendre les organes de direction plus responsables des stratégies de cybersécurité au sein des OSE.

- Il est important que la Commission reconnaisse que les membres des organes de direction des OSE et des entités importantes ont à leur disposition des équipes spécialisées dans la sécurité informatique, qui possèdent les qualifications nécessaires pour développer et mettre en œuvre des stratégies de cybersécurité. Il convient de se demander si les membres des organes de direction doivent suivre une formation ou si les rapports des RSSI (Responsable de la sécurité des systèmes d'information) ou des responsables de la sécurité informatique ne sont pas suffisants pour fournir aux membres des organes de direction des informations détaillées. Si la Commission considère qu'il est impératif que les membres des organes de direction suivent une formation en cybersécurité, nous l'enjoignons à partager des informations plus précises sur ce qu'entend la proposition concernant les « connaissances et compétences suffisantes ». Enfin, ces recommandations devraient être les mêmes dans toute l'UE afin d'éviter que les membres des organes de direction ne soient confrontés à des exigences divergentes.

Cryptage de bout-en-bout

La proposition prévoit des obligations pour certaines entités, d'adopter des technologies de renforcement de la sécurité. Par exemple, la proposition oblige les fournisseurs à adopter un cryptage de bout en bout afin d'améliorer la résistance des communications électroniques à la cybersécurité.

- Bien que nous soyons d'accord sur le fait que le cryptage de bout-en-bout offre un haut niveau de sécurité, il ne doit pas être imposé aux entreprises. Les entreprises devraient être autorisées à adopter les garanties et les mesures de sécurité qu'elles jugent appropriées.

- En outre, les Etats membres devraient mettre en place des moyens financiers et technologiques suffisants pour soutenir l'investissement dans de ces dispositifs, pour les entreprises qui n'auraient pas les moyens de se doter de ce type de solutions.

Notification des incidents

- L'article 30 de la directive propose de fixer le délai de notification des incidents aux autorités compétentes à 24 heures. Malgré la faible quantité d'informations demandées dans le cadre de ce premier signalement, le délai reste assez court. Dans les cas où le facteur temps est absolument clé, imposer aux opérateurs de communiquer des informations sur l'incident avant l'application de correctifs ou le rétablissement des opérations augmente la période pendant laquelle l'entreprise et ses clients sont vulnérables aux cyberattaques.

- Il conviendrait d'adopter une approche similaire à celle de du RGPD (Article 33), qui prévoit le signalement d'un incident sans retard excessif, et au plus tard dans les 72 heures. Cela permettrait d'assurer la cohérence entre les différents instruments législatifs de l'UE et davantage de clarté pour les entreprises.

- La Commission propose également d'inclure les menaces potentielles significatives ou les « quasi incidents » aux obligations de notification (Article 20 et considérant 55). Ceci pourrait entrainer une surcharge des notifications.

Gestion des risques

Conformément à l'objectif de la directive NIS de créer une culture de gestion des risques, et comme le souligne le Cybersecurity Act, NIS 2 devrait souligner le rôle continu de l'UE pour faciliter l'établissement et l'adoption de normes européennes et internationales pour la gestion des risques.

Formation et sensibilisation aux risques cyber

- Des cadres solides de gestion des risques jouent un rôle essentiel dans l'atténuation des menaces pour la cybersécurité. Pour aller plus loin, la proposition NIS 2 devrait proposer aux États membres de mettre davantage l'accent sur l'éducation et la sensibilisation aux risques et dans certains cas sur le financement des PME afin de les sécuriser.

- La période actuelle a coïncidé avec une meilleure compréhension par les entreprises des efforts qui doivent être réalisés en matière de sensibilisation aux risques, et la nécessité pour elles de disposer d'un minimal de sécurité. La médiatisation des cyberattaques et de leurs conséquences, ainsi que la meilleure publicité des actions par différents organismes (cybermalveillance.gouv.fr, organisations professionnelles, etc.) a permis de démocratiser le sujet auprès du grand public, y compris auprès des entreprises. Elles restent toutefois peu conscientes des mesures à prendre et sont parfois insuffisamment préparées. Les plus petites entreprises se considèrent souvent comme moins attractives pour les attaques que les plus grandes. Au sein de notre secteur, nous observons des niveaux de maturité très différents d'une entreprise à l'autre (de l'entreprise très peu sensibilisée à des degrés de forte appréhension de la cybersécurité). La prise de conscience a souvent lieu *a posteriori*, une fois que le risque se réalise.

- Le constat est clair : les entreprises sont confrontées à une pénurie de spécialistes qualifiés. Il est par conséquent nécessaire de renforcer l'attractivité des métiers de la cybersécurité, auprès des jeunes comme des publics en reconversion. Les programmes de formation initiale devraient être adaptées pour intégrer la cybersécurité, et les parcours de formation continue, notamment des dirigeants, devraient plus systématiquement être complétées par un module spécifique sur ces questions.

- En France, de nombreuses initiatives publiques et privées ont participé de cette prise de conscience (Cybermalveillance.gouv.fr, le dispositif national de sensibilisation, prévention et d'assistance aux victimes d'actes de cyber malveillance pour les particuliers, entreprises et collectivités territoriales). Dans ce cadre notamment, de nombreuses campagnes de sensibilisation sont menées, permettant de toucher des publics différents ; il faut également citer des initiatives comme le Mois européen de la cybersécurité, auquel participent de nombreuses organisations. Il est essentiel de poursuivre ces actions multiples et complémentaires.

Régime de supervision et sanctions

- La proposition prévoit des mesures d'audits sur site et d'autres mesures assorties de sanctions pouvant allées jusqu'à 2 % du chiffre d'affaires mondial en cas de non-conformité (Article 31).

Les sanctions proposées pourraient dissuader certains acteurs d'avoir recours à certains services, comme le cloud. De plus, la proposition exige de rendre publics les cas de non-conformité et d'infraction (Article 29(4)).

Normes de sécurité et gestion des risques

- Nous saluons la nouvelle approche plus complète de gestion des risques introduite par la Commission européenne. Il convient de tenir compte des normes européennes et internationales qui constituent une référence en matière de gestion des risques de cybersécurité et de protocoles utilisés pour la description des incidents. La Commission pourrait citer explicitement des normes précises en la matière pour remplacer les termes « technologies de pointes » dans la proposition.

Publication des vulnérabilités

- Plutôt qu'un rapport biannuel, l'ENISA pourrait publier, de manière régulière, des informations sur les vulnérabilités. Cela permettrait aux différents acteurs d'avoir un aperçu global de la situation et des menaces en temps réel.

[A propos de Syntec Numérique]
Syntec Numérique est le syndicat professionnel des entreprises de services du numérique (ESN), des éditeurs de logiciels et des sociétés de conseil en technologies. Il regroupe plus de 2 000 entreprises adhérentes qui réalisent 80% du chiffre d'affaires total du secteur (plus de 57 Md€ de chiffre d'affaires, 530 000 employés dans le secteur). Il compte 30 grands groupes, 120 ETI, 1 000 PME, 850 startups et TPE ; 11 Délégations régionales (Hauts de France, Grand Est, Auvergne Rhône-Alpes, Provence Alpes Côte d'Azur, Occitanie, Nouvelle Aquitaine, Pays de la Loire, Bretagne, Bourgogne Franche-Comté, Centre Val de Loire, Normandie) ; 20 membres collectifs (pôles de compétitivité, associations et clusters).
www.syntec-numerique.fr

[A propos de TECH IN France]
Créée en 2005, TECH IN France est une association professionnelle de loi 1901 qui a pour but de rassembler et de représenter les éditeurs de logiciels, de services internet et de plateformes en France. Porte-parole de l'industrie numérique, TECH IN France compte 400 entreprises adhérentes : de la startup à la multinationale en passant par la PME et les grands groupes français ; soit 8 milliards d'euros et 90 000 emplois. TECH IN France s'est donnée pour mission de mener une réflexion permanente sur l'évolution de l'industrie numérique et promouvoir l'attractivité du secteur.
www.techinfrance.fr