Global Security Mag
THE LOGICAL & PHYSICAL SECURITY MAGAZINE

Etes-vous « NIS » ou Not « NIS » ?

janvier 2019 par Polyanna Bigle, Avocate à la Cour d'appel de Paris, directrice du département Sécurité numérique de Lexing Alain Bensoussan Avocats

L'Union Européenne a construit collectivement « les conditions de sécurité indispensables à la transformation numérique de l'Union » avec la directive « NIS » en ayant pour objectif « d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information » dans chacun des pays de l'Union. La France a ainsi achevé de transposer la directive avec trois textes : la loi du 26 février 2018, un décret d'application du 23 mai 2018 et un arrêté du 13 juin 2018.

Quels acteurs sont concernés par les obligations de sécurité réseaux et systèmes d'information de la directive « NIS » dans droit français ?

Que recouvre la notion de « sécurité des réseaux et systèmes d'information » ? La loi prend soin de définir la « sécurité des réseaux et systèmes d'information » (SRSI) que certains dénomment cybersécurité. Elle consiste ainsi en « leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ».

Juridiquement, un « réseau et système d'information » est défini comme réseau de communication électronique et comme « tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques » ainsi que les données numériques elles-mêmes, « stockées, traitées, récupérées ou transmises » par réseaux et dispositifs, « en vue de leur fonctionnement, utilisation, protection et maintenance ».

La SRSI consiste donc en une résistance aux indisponibilités, compromissions d'authenticité et d'intégrité ou à la divulgation des données accessibles ou offerts par ces réseaux et systèmes, ou des services connexes. La nouveauté de la loi est de moduler la SRSI en fonction de niveaux confiance dont on peut penser qu'ils seront déterminés par décret d'application.

Quels sont les acteurs concernés ?

Il s'agit de nouvelles qualifications n'existant pas par ailleurs en droit français : les opérateurs de services essentiels et les fournisseurs de services numériques.

Opérateur de services essentiels. Tout d'abord, les opérateurs de services essentiels (OSE), qu'ils soient privés ou publics. Ils offrent des « services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture de leurs services ». Conformément à la Directive NIS, c'est le Premier Ministre qui fixe la liste. Après avoir recueilli les observations des opérateurs, il notifie à chaque OSE un arrêté de nomination. Les ministres et l'ANSSI peuvent également faire des propositions d'OSE.

Pour se reconnaitre, il existe une liste de services essentiels avec 16 secteurs d'activités : cela va de l'énergie, les transports, à la banque et services financiers, en passant par le social, la santé ou les infrastructures numériques.

Pour être OSE, il faut suffit de fournir au moins un de ces services « lorsque les réseaux et systèmes d'information sont nécessaires à la fourniture de ce service et qu'un incident aurait sur la fourniture de ces services des conséquences graves » appréciées selon 7 critères, comme par exemple la part de marché de l'opérateur ou la portée géographique.

Le 9 novembre 2018, l'ANSSI a annoncé qu'elle avait désigné 122 OSE et que cette liste serait mise à jour tous les ans.

Fournisseur de services numériques. Ce sont ceux fournissent des services payant par voie électronique et à la demande individuelle d'un internaute, sont les places de marché en ligne, les moteurs de recherche et les services d'informatique de Cloud (« en nuage »).

Toutefois, ne seront pas qualifiés de FSN au sens de la loi, les entreprises de moins de 50 salariés et dont le chiffre d'affaires annuel n'excède pas 10 millions d'euros. Être en dessous de ces seuils n'est pas pour autant une autorisation à faire n'importe quoi car, faut-il le rappeler, si des données personnelles sont traitées, le RGPD ne prévoit aucune exception aux obligations substantielles qu'il pose.

Le champ d'activité de ces opérateurs OSE et FSN est donc très large, que l'on soit client ou un prestataire. Le prestataire de cloud computing fait donc officiellement son entrée dans un texte légal, puisque qualifié de fournisseur de service numériques avec des obligations fortes.

Ne sont pas concernés par les textes les opérateurs de réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques pour les activités d'exploitation de réseaux et de fourniture de services de communication électronique ; les prestataires de services de confiance visés par le Règlement eIDAS ; les opérateurs d'importance vitale, mais uniquement pour la partie de leur activité soumise aux exigences sectorielles équivalentes à la présente loi. Que doivent faire ses acteurs concernés ?

- Déclarer à l'ANSSI une liste tenue à jour annuellement une liste des réseaux et systèmes d'information nécessaires à la fourniture de leurs services. Elle doit comprendre la liste des réseaux et systèmes d'information exploités par un tiers en externalisation. Ceci implique donc que le tiers fournisse ces éléments lors de la conclusion du contrat.

- Déclarer à l'ANSSI la personne chargée de les représenter auprès de l'ANSSI : celle-ci est responsable du respect des obligations légales.

- Se mettre en conformité, à ses frais, à des règles ayant pour objectif de garantir un certain niveau de sécurité qui sera fonction du risque existant et de l'état des connaissances.

o Pour les OSE, les règles sont fixées par le Premier Ministre autour de : □ la gouvernance de la SRSI (PSSI et homologation de sécurité des réseaux et SI), □ la protection de l'architecture et de l'administration et le contrôle d'accès des réseaux et des réseaux et systèmes d'information, □ la détection des incidents et le traitement des incidents de sécurité affectant les réseaux et systèmes d'information □ pour la résilience des activités, la gestion de crises d'incidents de sécurité ayant un impact majeur sur des services essentiels.

On se rapproche ici sans étonnement des exigences posées par le RGPD en matière de données personnelles. Mais le Premier Ministre pourra exiger de recourir à des dispositifs matériels ou logiciels ou services informatiques certifiés. Un schéma directeur relatif à la sécurité est donc avant tout nécessaire pour suivre la bonne direction.

o Pour les FSN, le décret d'application fait un renvoi vers le règlement d'exécution n°2018/151 du 30 janvier 2018 portant modalités d'application de la directive NIS. Cela implique d'identifier les risques qui menacent la sécurité de ces réseaux et systèmes d'information et de prendre les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer ces risques.

A noter que le FSN doit tenir à disposition de l'ANSSI, outre sa liste précitée, « les documents permettant de vérifier la mise en œuvre » des mesures de sécurité exigées par l'article 12 de la loi … on ne peut là encore s'empêcher un parallèle avec le principe d'accountability du RGPD pesant sur les responsables de traitement. Mais la différence est de taille : le périmètre de NIS (réseaux et systèmes) n'est pas le même que celui du RGPD (données personnelles). Les documents devront ainsi prévoir un chapitre sur la mise en œuvre des mesures de sécurité au titre de NIS, et un chapitre sur celles au titre du RGPD.

- Déclarer à l'ANSSI, sans délai, les incidents de sécurité significatifs. Il s'agit des incidents qui ont ou risquent d'avoir « un impact significatif sur la continuité de ces services » et ce, en fonction du nombre d'utilisateurs et de la zone géographique touchés et de la durée

de l'incident. A charge pour l'ANSSI d'en informer ou pas le public « lorsque cette information est nécessaire pour prévenir ou traiter l'incident » et éventuellement les autres autorités des Etats membres de l'Union Européenne. Le cas échéant, l'ANSSI veillera à ne pas divulguer d'informations risquant de porter atteinte à la sécurité et au secrets commerciaux et industriels de l'opérateur.

- Se soumettre au contrôle de l'ANSSI décidé par le Premier Ministre. Ces contrôles seront contradictoires selon une convention conclue avec l'ANSSI. Ils se feront sur pièce et sur place soit par un agent de l'ANSSI, soit par un prestataire de service qualifié qu'elle aura désigné. La différence pourrait être de taille car que le coût jour/homme d'un contrôle mobilisant un agent public est fixé par arrêté, le coût des contrôles effectué par un prestataire est déterminé librement par les parties… et c'est l'opérateur qui devra payer les coûts de contrôle. L'effet dissuasif d'un contrôle est non négligeable, d'autant qu'un contrôle de l'ANSSI pourrait mécaniquement entraîner un contrôle de la CNIL et vice et versa…

L'ANSSI va accompagner les OSE dans la mise en œuvre de leur dispositif de cybersécurité pour assurer leur protection. Rien n'est cependant annoncé pour les FSN.

Comment faire ses déclarations ? Un formulaire est disponible sur le site « https://www.ssi.gouv.fr/ » pour chacun de ses réseaux listés de même qu'un formulaire de déclaration d'incident.

Quelles sont les sanctions ? L'ANSSI dispose d'un pouvoir de sanction de l'échelle de la mise en demeure jusqu'à des peines amendes allant pour les OSE jusqu'à 125 000 euros et pour les FSN, 100 000 euros.

On pourra bien entendu former un recours administratif auprès du Premier Ministre contre une décision de l'ANSSI, puis éventuellement un recours contentieux.

Quels sont les impacts sur les contrats avec ces acteurs ?

Les textes sont muets sur les obligations contractuelles de ces acteurs. Néanmoins, un client pourra d'une part exiger contractuellement de son prestataire qu'il se conforme à ces exigences : même si surabondant pour ceux qui sont soumis à la loi, les dispositions peuvent faire office de référentiel ou d'état de l'art à valeur légale pour ceux qui n'y sont pas soumis.

D'autre part, il pourra exiger contractuellement la documentation prouvant que l'OSE ou le FSE atteint ces exigences de sécurité – dans la limite liée à la confidentialité nécessaire à la protection des réseaux et des systèmes d'information. Les labels, qualifications et certifications auront là un rôle majeur.

Pour conclure, l'arsenal législatif et réglementaire « NIS » s'inscrit dans le cadre général posé par le code de la sécurité intérieur selon lequel « : La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ». Ici, la SRSI trouve une définition légale…s'imposant aux activités majeures du numérique et des communications électroniques.

Polyanna Bigle – Directeur du Département Sécurité Numérique Cabinet Alain Bensoussan – Lexing

---

POUR ALLER PLUS LOIN

Directive 2016/1148 du 6 juillet 2016 « Network and information Security » sur la sécurité des réseaux et des systèmes d'information. Loi 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité Décret 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Trois arrêtés du 13 juin, 1er août et 14 septembre 2018 fixant :
- les modalités des déclarations prévues aux articles 8, 11 et 20 du décret 2018-384 ;
- le coût d'un contrôle effectué par l'ANSSI en application des articles 8 et 14 de la loi 2018-133
- les règles de sécurité et les délais mentionnés à l'article 10 du décret 2018-384