Renaissance Numérique

AVRIL 2024

NOTE

7 recommandations sur le projet de loi de transposition de la Directive NIS2

Renaissance Numérique

3 avril 2024

7 recommandations sur le projet de loi de transposition de la Directive NIS2

Table des matières

Le contexte

La Directive NIS2 (*Network and Information Security*)[1] constitue une avancée majeure du normatif européen dans le domaine de la cybersécurité. Contrairement à sa prédécesseure, NIS2 établit un cadre clair, précis et harmonieux d'amélioration de la posture de maturité en cybersécurité des organisations.

NIS2 insiste sur le besoin pour les États membres de structurer et outiller leur approche de lutte contre les cybermenaces *via* l'élaboration d'une stratégie nationale et la création ou désignation d'autorités nationales compétentes et d'équipes opérationnelles de réponse à incident. NIS2 soutient une approche holistique en termes a) de périmètre en établissant différents critères de désignation des entités concernées ; et b) de responsabilité de cybersécurité à travers un "cœur" de mesures concrètes. Ainsi, la responsabilisation des acteurs concernés passe par une approche par les risques devant être déployée activement et par l'attribution de la charge de la preuve aux entités concernées.

Lorsqu'il s'agit des mesures concrètes, NIS2 a grandement évolué par rapport à sa prédécesseure. La Directive énumère 10 mesures concrètes, dont notamment une attention particulière portée à la sécurité des fournisseurs. En outre, la Directive s'attache à promouvoir une compréhension partagée de l'état de la menace à travers un processus cadré de signalement d'incidents de cybersécurité. Les débats entre les colégislateurs ayant animé la rédaction de cette exigence ont grandement contribué à lui donner une temporalité et une proportionnalité bénéfiques aussi bien pour les entités concernées que pour les autorités compétentes qui recevront ces notifications.

Enfin, il est également salutaire de voir que des leçons ont été apprises de NIS1. Ainsi, le changement de braquet en ce qui concerne la couverture des systèmes d'informations (SI) des entités concernées dans leur globalité sera fructueux en permettant une approche raisonnable et globale à l'échelle de l'organisation. De même, NIS2 précise également ses articulations avec d'autres textes, tels le Règlement DORA[2] ou encore la Directive REC[3]. Même si l'étude d'impact ignore certains secteurs d'activité, on peut d'ores et déjà se concentrer sur leur nécessaire prise en compte dans une démarche de résilience et dans une stratégie nationale.

---

[1]. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 sur les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union https://eur-lex.europa.eu/eli/dir/2022/2555

[2]. Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554

[3]. Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2557

Sur l’esprit de la Directive

Créer une stratégie nationale

Afin d’asseoir l’esprit de collaboration et de maturité harmonieuse, il importe à ce que les autorités se saisissent de l’occasion pour produire une stratégie nationale unifiée de cybersécurité et cyberdéfense. Cette stratégie serait également l’occasion de préciser le rôle de l’Agence nationale de la sécurité des systèmes d'information (ANSSI) et les interactions avec d’autres administrations, notamment indépendantes, en France ; précision nécessaire vu les attentes de la communauté, d’une part, et la diversité de textes européens aux degrés d’avancement hétérogènes, de l’autre.

Cette stratégie nationale est l’outil principal pour prendre la mesure du sujet porté par NIS2 : l’effort de protéger ce qui assure le fonctionnement et le développement de l’Union doit être un effort coordonné, pris à bras le corps par les dirigeants et bénéficiant de leur appui politique. Nous déplorons ainsi un projet de transposition qui n’est pas à la hauteur de cet enjeu, le texte faisant vaguement allusion à cette ambition structurante de NIS2.

Promouvoir la responsabilité de la direction d’une organisation

Dans son article 20, NIS2 fait la part belle à la gouvernance de la cybersécurité. Ainsi, les États membres veillent à ce que les organes de direction des entités essentielles (EE) et importantes (EI) :

- approuvent les mesures de gestion des risques de cybersécurité prises par ces entités afin de se conformer à l’article 21,
- supervisent sa mise en oeuvre,
- puissent être tenus responsables de la violation dudit article par ces entités.

C’est dans cet esprit que NIS2 insiste sur la nécessité pour les membres des organes de direction des entités concernées à prendre leurs responsabilités, combattant la solitude bien connue de l’opérationnel de cybersécurité.

Toujours dans son article 20, NIS2 insiste pour que les États membres veillent à ce que les organes de direction des entités essentielles et importantes soient tenus de suivre une formation. Ils encouragent les EE et EI à offrir régulièrement une formation similaire à leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l’entité.

Nous regrettons donc que le projet de transposition et la démarche adoptée par l’ANSSI abaissent cet enjeu, renvoyant l’approche générale de prise en compte au plus haut niveau

de la prise de décision à un sujet purement opérationnel de mesures techniques obligatoires à déployer. Cet abaissement de l'ambition risque de dévoyer les efforts faits depuis des années par de nombreux responsables de cybersécurité auprès de leur hiérarchie et va à l'encontre d'une compréhension déjà acquise de la part de nombreux acteurs (assurances, financiers, etc.) du besoin d'intégrer le risque cyber dans les risques stratégiques d'une organisation, qui doivent être pris en compte au plus haut niveau.

Les besoins saillants

Clarifier le périmètre d'application

De façon générale, NIS2 permet en grande partie aux organisations de se répartir entre EE et EI. Il reste quelques éclaircissements complémentaires que le projet de transposition devrait apporter.
Dans certains cas, il est difficile d'identifier si une entité est incluse dans le périmètre de NIS2. Il s'agit par exemple des fournisseurs d'EE ou encore des ESN (entreprises de services numériques). De plus, il est nécessaire de clarifier le périmètre d'assujettissement à NIS2 dans le cadre d'une distinction "activité principale/activité partielle" au sein d'une grande entreprise.

Le projet de transposition tel que rédigé au 3 avril met énormément l'accent sur l'intégration de la Directive REC. Il est bienvenu de tendre à l'harmonisation des différents cadres normatifs, surtout lorsqu'ils ont une complémentarité.

Cependant, le volet de transposition relatif à NIS2 est sous-optimal : le texte du projet mélange Organismes d'importance vitale (OIV) et EE/EI sans établir une articulation claire. Conséquemment, cette distinction réintroduit la notion de "Système d'Information d'Importance Vitale", alors que cette notion a été supprimée de NIS2 pour prévenir le morcellement de périmètres opérationnels à protéger.

En conclusion, nous sommes préoccupés par l'approche par décret, proposée par le projet de loi. Non seulement celui-ci n'apporte pas les éclaircissements nécessaires (pas si nombreux d'ailleurs), mais en plus il fait machine arrière par rapport à la directive en décidant de confier l'identification des entités concernées à l'exécutif. En effet, le texte du projet de loi est déséquilibré en ce qu'il enlève la clarté remarquable de NIS2 pour introduire une approche par décret. Si cette approche était entendable avec NIS1, elle l'est bien moins aujourd'hui : le texte de NIS2 est bien plus clair, structuré et concret que NIS1. Nous nous étonnons donc de cette démarche de gouvernance généralisée par décrets dans une situation qui ne le nécessite pas.

Clarifier les interactions entre les entités concernées et l'ANSSI

Dans le cadre de NIS2, l'ANSSI est très légitime à être l'organe de contrôle de conformité. De plus, certaines informations (telles que les notifications d'incidents par ex.) doivent y être signalées. Ainsi, l'ANSSI devrait changer de dimension et accueillir dans son giron des entités concernées qui n'ont pas la même culture de la cybersécurité et de la gestion du risque systémique que les OIV. C'est le cas notamment des collectivités locales de moyenne importance, qu'il n'est pas possible de traiter comme une entreprise.

Enfin, le projet de transposition fait la place belle à un contrôle étendu de la part de l'exécutif par le truchement de l'ANSSI, allant ainsi bien plus loin dans la démarche de contrôle présentée dans NIS2 (REC et DORA aussi). L'ANSSI se verrait ainsi enrichie de pouvoirs étendus, la poussant ainsi à changer de culture et de façon d'agir. Des changements culturels et organisationnels qui interrogent sur les capacités des moyens humains à évoluer dans la même temporalité. Il convient d'anticiper et cadrer cette évolution pour limiter l'émergence d'un super-pouvoir contraignant et doté de capacités de sanction.

Pour toutes ces raisons, il est essentiel de comprendre quelle serait la profondeur des interactions entre les entités concernées et l'ANSSI.

Partage d'information

1) **La difficulté de faire émerger une organisation (avec ses besoins de cyber et sa structure propre) alors que la Directive parle d'entité**

L'organisation de la cybersécurité diffère considérablement d'une entité à une autre, étant influencée par la structure et la gouvernance du système d'information (SI). La structure opérationnelle peut être monolithique, fragmentée, entièrement internalisée, externalisée ou hybride, selon la complexité de l'organisation. Par exemple, la défense d'un SI central sera différente de celle d'un SI fragmenté composé de plusieurs SI indépendants et plus ou moins interconnectés. Dans les entreprises internationales, la géographie joue un rôle important, avec des systèmes d'information et de défense potentiellement segmentés par entité, région ou pays. Tous les modèles d'organisation sont possibles et doivent être adaptés au mieux à la structure du SI.

Si les modèles d'organisation de la cybersécurité peuvent refléter le découpage en entités juridiques, cela est plus fréquent dans les petites et moyennes entreprises. Dans les grandes organisations, l'organisation de la cybersécurité est souvent décorrélée des entités juridiques, et l'équipe cyber peut ne pas être familiarisée avec celles-ci. Il est important de noter que les entités juridiques peuvent être nombreuses et en constante évolution, sans lien direct avec la gouvernance cyber.

RECOMMANDATION 1

Sur le volet de la cybersécurité opérationnelle, nous encourageons à ce que la description de l'organisation, du point de vue de la cybersécurité, soit laissée à l'appréciation de l'organisation EE ou EI pour refléter la réalité opérationnelle.
Cette recommandation s'impose d'autant plus que le projet de transposition introduit une confusion significative dans la qualification des entités concernées, rendant encore plus difficile l'adoption opérationnelle. La réintroduction artificielle de typologies d'entités et de SI nuit gravement à la résilience et le déploiement de mesures efficaces.

2) Le contact principal de l'ANSSI avec une organisation visée par NIS2

Pour des petites ou moyennes organisations ou pour des grandes organisations qui ont un SI et une cybersécurité centralisée, le contact privilégié pourrait être le responsable cybersécurité ou son pendant opérationnel.

Pour les organisations avec modèles opérationnels de cybersécurité hétérogènes, différents rôles peuvent émerger, chacun avec une responsabilité cadrée (*e.g.*, un directeur cybersécurité, un responsable opérationnel, un *Computer Security Incident Response Team* (CSIRT) - ou un centre d'alerte et de réaction aux cyberattaques -, avec astreintes et une habilitation de déclaration d'incidents, etc.). Dans ces cas complexes, l'organisation pourrait fournir des coordonnées de contact pour ces différents types d'interlocuteurs, avec un contact principal et un ou plusieurs contacts secondaires, nominatifs et/ou joignables *via* des coordonnées génériques.

3) La fluidité du partage d'information est un besoin pressant

Il est entendu que l'ANSSI collecterait de nombreuses informations sensibles quant à des incidents en cours et vulnérabilités devant être corrigées, chez un grand nombre d'organisations. Toutefois, peu d'éléments sont disponibles quant à la façon dont l'ANSSI ferait un "partage descendant" pour améliorer la compréhension opérationnelle des acteurs quant au paysage de la menace.
Plus spécifiquement, beaucoup d'organisations regrettent que ce partage d'information ne soit pas en place aujourd'hui, dans une coopération maîtrisée, avec une gestion appropriée des secrets. Dans le cadre de NIS2 et l'évolution du rôle de l'ANSSI, il est donc primordial que l'Agence joue un rôle pivot dans la communication sur les incidents auprès des organisations concernées, en protégeant bien sûr leur identité, sauf si celles-ci autorisent expressément la levée de l'anonymat dans certains cas particuliers.

Le rôle et les prérogatives de l'ANSSI étant amenés à évoluer, il importe de donner le mandat et les moyens à l'ANSSI de recruter et de s'outiller pour procéder efficacement à la supervision requise. Cependant, l'Agence ne peut raisonnablement concentrer des pouvoirs de supervision et sanction administrative sans aucun contrôle indépendant. En effet, le projet de loi de transposition gomme la distinction entre EE et EI en termes de sévérité des contrôles, mettant des entités à l'importance différente sur pied d'égalité en matière de preuve de conformité. Plus délicat encore, les pleins pouvoirs sont donnés à l'ANSSI sans qu'aucun mécanisme de contrôle indépendant n'existe. Il est utile de rappeler que, contrairement à l'Arcep ou la CNIL, l'ANSSI n'est pas une autorité administrative indépendante, mais dépend du Premier ministre. L'existence d'une commission des sanctions, rattachée au Premier ministre, dont c'est la seule fonction, ne paraît pas être une garantie suffisante, pour qu'un contrôle réellement indépendant soit effectué.

Le texte prévoit également des obligations d'informer l'ANSSI de la cession d'entité importante, avec un délai de prévenance de six mois, qui n'est pas toujours possible de tenir. Le cas de l'avenir d'Atos illustre bien le caractère délicat de ce délai, et pose aussi la question de l'acheteur, qui n'est pas traité directement, et doit s'articuler avec d'autres dispositifs existants.

Identifier et notifier les incidents de cybersécurité

1) Identifier les incidents significatifs : des critères de qualification spécifiques sont nécessaires.

La Directive NIS2 fournit une bonne définition générale de ce qu'est un incident significatif en portant sur l'impact des dégâts[4]. Celle-ci mériterait d'être clarifiée dans le texte de transposition pour préciser les façons de qualifier l'impact.
Pour le qualifier, il convient de pouvoir ramener cet impact au périmètre concerné. En effet, un impact important sur une petite ou moyenne entreprise peut signifier une atteinte à sa pérennité. Dans le cas d'une grande entreprise, certains incidents ayantun impact significatif peuvent rester circonscrits à une seule entité de l'organisation. Dans ce cas, l'impact est important pour cette entité sans forcément l'être pour la grande entreprise dans son ensemble.

Parmi les impacts importants sur une entreprise, il convient de prendre en compte :

- Les impacts directs de perte d'activité ;
- Les coûts de gestion de l'incident (diagnostic, remédiation, communication, gestion contractuelle et juridique) ;
- Les coûts de reconstruction ou retour à un fonctionnement nominal ;

[4]. Voir Art. 6 (6) et (7) pour les définitions générales et Art. 23 (3) de la Directive pour la qualification d'un incident significatif.

- Les impacts réputationnels, la perte de contrats, la perte d'opportunités et les risques contractuels et réglementaires.

RECOMMANDATION 2

Nous recommandons l'addition d'un critère d'importance de l'incident qu'un incident non connu du Comité exécutif/Comité de direction n'est pas un incident significatif.

RECOMMANDATION 3

Nous recommandons la co-création de groupes de critères par secteur concerné. Ainsi, lorsque les acteurs du secteur de l'énergie par exemple prendront l'attache de l'ANSSI, ils peuvent transmettre leurs définitions et critères de qualification d'incident significatif. Les acteurs de la santé, des administrations publiques concernées, etc. en feront de même. Cette approche permettrait une compréhension fine et au plus près de la réalité, rendant possible un accompagnement adapté par l'ANSSI.

2) Notifier les incidents significatifs touchant les entités concernées

La Directive établit un processus clair et structuré de notification des incidents significatifs à l'autorité nationale, avec un premier signalement dans les 24 heures après avoir constaté l'incident, puis la transmission d'éléments techniques résultant des investigations dans les 3 jours suivants et, enfin, la transmission d'un rapport dans le mois qui suit la clôture de l'incident. La temporalité des notifications est donc équilibrée par rapport aux besoins opérationnels. En effet, lorsqu'un incident significatif survient, sa gestion nécessite une mobilisation importante afin d'éviter qu'il se transforme en crise d'origine cyber. Chaque heure, chaque minute compte pour organiser les différentes actions d'investigation et les mesures de remédiation. Ainsi, l'approche par étapes introduite par NIS2 reflète bien la prise en compte du temps et des ressources consacrés à gestion de l'incident.

Nous sommes ainsi préoccupés par l'approche profondément divergente décrite dans le projet de loi de transposition. La notification de tout incident *"ayant un impact sur la fourniture des services"* de l'entité concernée doit se faire *"sans délai"*.
D'une part, cette définition déborde de la définition d'un incident de cybersécurité. D'autre part, l'injonction de signaler *"sans délai"* risque de constituer une gêne à la gestion de l'incident, dont la performance est cruciale pendant les premiers jours. Une telle approche comminatoire transforme la notification d'un incident en obstacle et fardeau là où, au démarrage d'un incident d'une telle ampleur, toute l'énergie doit être consacrée à la remédiation et *a minima* la non-aggravation de la situation.

RECOMMANDATION 4

Nous recommandons donc la rationalisation des approches de signalement :

- Pour optimiser les temps de déclaration, les personnes autorisées à faire cette déclaration doivent être préalablement enregistrées par l'organisation auprès de l'autorité.
- La temporalité de déclaration de NIS2 doit être reprise en l'état. Le projet de transposition devrait, par le truchement d'un décret si plus pratique, inclure les éléments demandés à chaque étape.
- Pour assurer une efficacité et une cohérence dans la gestion des incidents de cybersécurité au niveau européen, il est crucial que les processus de notification soient harmonisés et standardisés, avec des échéances et des informations communes à renseigner. Cela permettra aux entreprises internationales de signaler un incident important à une seule autorité NIS2, et d'éviter ainsi les déclarations multiples et potentiellement contradictoires.

Mesures de sécurité et gestion des tiers

A l'heure actuelle, le projet de loi de transposition omet la mention des mesures de sécurité prévues dans NIS2. Le texte laisse la place à une mention vague de décret à venir qui les préciseraient. Cependant, une proposition de 20 mesures élaborées par l'ANSSI a déjà été diffusée auprès de différents acteurs de la communauté. Il est ainsi possible de voir la logique qui s'en dégage. Alors que la formulation des mesures est plutôt claire et compréhensible, la question subsiste quant à la cohérence de ces mesures avec celles d'autres pays européens.

RECOMMANDATION 5

Nous recommandons une déclinaison raisonnable des mesures déjà existantes dans NIS2 afin d'éviter un dévoiement du caractère européen de ce texte une fois transposé en France et les difficultés associées à une contextualisation nationale trop prononcée.
Une préoccupation principale est la sécurité des tiers. Notamment, il est mentionné dans l'avant-projet de loi que celle-ci sera gérée aux moyens de contrats. Cette approche risque d'introduire une myopie significative : en pratique, les incidents liés aux tiers sont très nombreux. Ce processus de révision des contrats risque d'être lourd, long et coûteux, et donc source de mécontentement et d'insécurité.

RECOMMANDATION 6

Nous recommandons la création et la dissémination de clauses contractuelles standard pour aborder le socle du volet contractuel.

RECOMMANDATION 7

Nous recommandons un travail de clarification dédié aux services cloud. A l'heure actuelle, ceux-là sont totalement absents des textes. Or et notamment concernant les services SaaS qui sont, par construction, des services mutualisés destinés à différents clients et à utiliser « tels quels », des mesures génériques ou les seules CGU sont largement insuffisantes et inadaptées.

AUTEURS

Rayna Stamboliyska, Présidente, RS Strategy

Samuel Le Goff, Directeur conseil, Commstrat ; Vice-président de Renaissance Numérique

À propos

Créé en 2007, Renaissance Numérique est un think tank indépendant dédié à la transformation numérique de la société. Il œuvre à éclairer les évolutions que cette transformation entraîne et à donner à chacun les clés de sa maîtrise.
Renaissance Numérique est un lieu de débat et de confrontation positive d'expertises et d'idées. Il réunit des universitaires, des personnalités, des organisations non gouvernementales ou encore des entreprises. Ses réflexions, largement diffusées via des contributions, publications et des événements, sont portées auprès d'acteurs publics comme privés, au niveau français, européen et international.

Renaissance Numérique est membre de l'Observatoire de la haine en ligne porté par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et du comité d'organisation du Forum sur la Gouvernance de l'Internet (FGI) France.

Retrouvez nos publications sur :
www.renaissancenumerique.org

Renaissance
Numérique

Renaissance Numérique

Koburo, 35 rue Chanzy – 75011 Paris
www.renaissancenumerique.org

Novembre 2024