Directive NIS : les bons vœux de l'ANSSI

Elise BRUILLON

Directeur, Responsable des offres « Conformité » et « Prévenir »
FORMIND

En date du 28 octobre 2020, l'ANSSI publiait sur son site une actualité dénommée « Révision de la directive NIS[1]: une opportunité pour renforcer le niveau de cybersécurité au sein de l'UE » ; cette information relayée par les médias sociaux a paradoxalement suscité très peu de commentaires.

Pourtant, le sujet touche la majorité des secteurs d'activité de notre économie et nombres d'acteurs sont en cours de constitution des dossiers d'homologation de leurs systèmes d'information essentiels (SIE) auprès de l'agence.

Dans cette actualité, l'ANSSI appelait de ses vœux à une harmonisation sur la plaque européenne des pratiques relatives à la gouvernance des risques numériques et à une coopération transfrontalière plus développée; elle mettait également en avant la nécessité de placer comme axe d'étude les attaques par rebond sur les chaines de valeur des Opérateurs de Services Essentiels (OSE) notamment en conseillant de maitriser l'ensemble des interventions directes et/ou indirectes des tiers (fournisseurs, partenaires etc…) sur les SIE.

Simple positionnement de notre agence française ou *Gentle reminder* à l'adresse de l'ENISA, cette actualité nous semble intéressante sur trois axes dans le secteur de la cyber conformité.

La Directive NIS détermine un objectif commun de sécurité

L'Union européenne a pris le parti de protéger son marché économique via le renforcement des capacités en cybersécurité des Etats et d'acteurs spécifiques comme les entreprises ou organismes publics identifiés dans des secteurs clés. Ces secteurs clés sont qualifiés de « services essentiels » au fonctionnement de l'économie et de la société. Ces acteurs sont généralement tributaires d'un ou plusieurs systèmes d'information dits *essentiels (SIE)*. L'objectif est donc de pouvoir gérer les interfaces et dépendances à ces SIE lorsque ce produit un évènement de sécurité.

Pour ce faire, la Directive NIS pose le cadre de coopération entre Etats Membres notamment par

[1] Pour (Network and Information System Security)

le renforcement de leurs capacités en matière de cybersécurité ; la désignation d'autorités nationales compétentes en matière de cybersécurité et de centres de réponse aux incidents de sécurité ; l'instauration de règles communes avec notamment la notification des incidents, le partage des informations techniques sur les risques et les vulnérabilités.

Sur ce troisième volet relatif aux règles communes, l'ANSSI se réjouissait de ces compléments nécessaires à notre réglementation nationale relative aux activités d'importance vitale ; la Directive NIS confortait les orientations stratégiques de l'ANSSI dans son positionnement d'autorité nationale compétente en la matière et adoubait les CSIRT comme un maillon essentiel de la chaine de protection. Elle fixait dans le marbre les objectifs de sécurité pour converger vers une protection commune sans frontières.

Pour rappel, cette remontée d'information des incidents nationaux pour un partage européen via les agences de sécurité concernées, reprenait l'orientation prise dans le secteur des communications électroniques avec la notification des incidents de sécurité[2] et la consolidation de ce reporting au niveau de l'ENISA.

L'ANSSI améliore sa connaissance de notre écosystème cyber en consolidant sur l'ensemble des secteurs d'activités économiques un ensemble informationnel de premier choix pour anticiper, prévenir et se protéger des attaques.

Par conséquent, la Directive NIS permettait de cadrer une priorité transverse européenne telle que mettre sous contrôle les attaques sur les services essentiels d'une nation et faire en sorte que cet objectif puisse être décliné chez tous nos partenaires européens en fixant des moyens et des ressources.

L'ANSSI a personnalisé la transposition de la Directive NIS en rendant incontournable l'analyse de risques

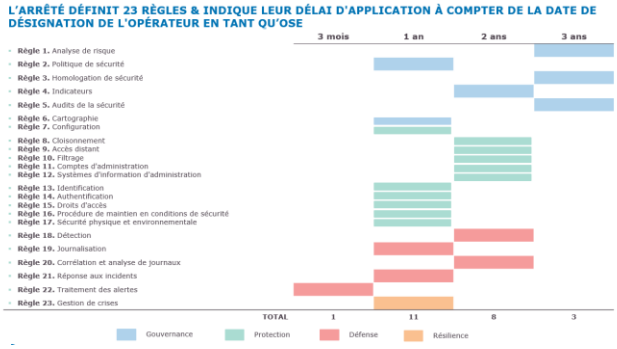
Pour pouvoir être appliquée dans une législation nationale, une directive doit d'être transposée en droit national via un véhicule législatif. La transposition laisse la possibilité pour chaque état de personnaliser la vision de l'objectif de sécurité et des moyens pour y parvenir. Chaque état est souverain dans la manière de transposer législativement la Directive pourvu que se retrouvent les grands axes fournis par le texte européen.

Ainsi la Directive NIS[3] a été transposée en droit français sous l'étroit contrôle de l'ANSSI ; le décret d'application de la loi de transposition au Journal Officiel, a été publié le 25 mai 2018 et identifiait les principaux secteurs concernés tels que représentés ci-dessous :

Au sein de ces secteurs d'activité, l'ANSSI a désigné 122 OSE, cette liste classifiée reprend *stricto sensu* les consignes de la Directive. Les OSE doivent mettre en œuvre 23 mesures techniques et organisationnelles pour gérer les risques menaçant la sécurité des réseaux et des systèmes d'information. Ces 23 mesures font partie de l'arrêté du 14 septembre 2018 qui illustre l'interprétation par l'ANSSI de la Directive NIS.

[2] Code des Postes et Communications électroniques

[3] DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne.



En France, la Directive NIS est transposée de manière réglementaire en 23 règles, 4 thématiques et une logique de boucle d'amélioration continue. L'acte fondateur de la mise en conformité des OSE commence par la réalisation d'une analyse de risques qui est une pièce incontournable du dossier d'homologation.

Dans la communauté cybersécurité, il est entendu que l'étude, la qualification du risque, et son affinage est un travail de séquencement avec encore beaucoup (trop ?) de subjectivisme et d'empirisme.

En effet, la profondeur d'une analyse de risques dépend du profil de son rédacteur fonctionnel versus technique, de ses expériences, de sa connaissance de véritables incidents de sécurité. Ce pourquoi il est nécessaire de limiter cette part de subjectivisme en adoptant une démarche commune d'analyse généralement définie par une autorité régalienne. Ainsi, la méthodologie d'analyse de risques consacrée en France en 2021 est Ebios RM. L'ANSSI a dépoussiéré la méthodologie EBIOS 2010 pour permettre de disposer d'un outil plus adapté à la menace actuelle.

La Directive NIS n'avait pas vocation à cadrer les analyses de risques, ce n'est pas la vocation d'un instrument législatif qui poursuit des objectifs plus stratégiques : maitriser les services essentiels d'une nation.

Dès lors, si nous nous plaçons sur un terrain de jeu européen, l'absence d'une méthodologie commune à l'ensemble des Etats de l'Union ne permet pas de disposer d'une vision comparable des risques pesant sur les services essentiels.

Ces derniers sont issus de différentes méthodologies nationales et ce mal nécessaire (subjectivisme +empirisme dans la réalisation des analyses de risque) rend la vision plus trouble du risque pesant sur les SIE et sans garantie de fiabilité alors que la chaîne de valeur à protéger reste la même.

Comparer les risques consolidés au niveau européen pour en tirer des orientations stratégiques de protection et de défense nécessite donc d'harmoniser nos manières de réaliser nos analyses de risques. Et ce point particulier n'a pas échappé aux fourches caudines de l'ANSSI.

Une méthodologie à imposer pour harmoniser les pratiques ?

Si tous nous partageons cette vision d'un risque affranchi des frontières matérielles ayant des effets sur des secteurs similaires ou semblables ; au sein de l'Union européenne notre démarche d'analyse n'est pas forcément la plus harmonieuse. Si la norme ISO 27005, nous fournit des lignes directrices pour réaliser une telle étude, chaque agence nationale a décliné sa propre méthodologie pour identifier des objectifs de sécurité conformes à ses lignes directrices de défense et de résilience.

Or pour se protéger de manière commune, il convient de s'entendre et de partager sur comment nous allons qualifier ces fameux risques sur les services essentiels et quel est le séquencement logique le plus efficace pour que

l'étude puisse aboutir à un résultat probant et comparable entre états.

Par conséquent, l'harmonisation des pratiques pour dérouler l'étude de risques nous semble légitime et pertinente. La question provocante est que nous apporte EBIOS RM dans ce contexte si particulier de la conformité NIS ?

Tous nous avons salué le formidable dépoussiérage de la méthodologie et la réalisation d'atelier collaboratif et itératif permettant d'embarquer les métiers rétifs à l'exercice. Et pourtant, nous avons hurlé à la mort sur le fait que les sources de menaces non intentionnelles n'étaient pas prises en compte dans un tel exercice. Nous nous sommes cassé les dents sur le détourage des parties prenantes et des chemins d'attaques en nous référant frénétiquement à la base de connaissances.

Néanmoins, dans le cadre particulier de la mise en conformité aux 23 règles d'un OSE, ce déroulement de l'analyse nous permet de changer le prisme de notre vision du risque. Le métier parle, s'approprie les concepts et nous oblige à challenger nos connaissances et notre vision prêt à l'emploi d'une attaque. De notre opinion, EBIOS RM nous permet de nous placer dans le dispositif d'une attaque probablement réelle et de disposer d'un outil de synthèse pour communiquer auprès des instances managériales d'un OSE.

Et c'est bien le sens de ces 23 règles, connais ton écosystème et tes vulnérabilités, corrige les autant faire se peut et sache informer au bon moment tes autorités comme le ferait tout agent d'un maillage plus vaste que son propre écosystème.

Dès lors, la suggestion de l'ANSSI d'harmoniser les pratiques de gouvernance des risques numériques semble étroitement liée à l'harmonisation de la méthodologie d'analyse de risques qui reste le premier maillon d'une saine gouvernance des risques.

Pour conclure, il nous semble que ce qui ferait la force d'une harmonisation dans le cadre de la directive NIS serait la vision commune de l'appréhension du risque, de sa qualification à son nécessaire arbitrage. Si la multiplication des attaques par rebond doit être pris en compte de manière plus prégnante selon l'Agence, cette menace n'est pas nouvelle et certaines autorités administratives indépendantes (ACPR, CNIL…) avaient déjà pris le parti de consolider les exigences de sécurité sur la maitrise des tiers dont les actions portaient incidence sur la sécurité du SI. Le Règlement Général relatif à la Protection des Données impose la maîtrise des sous -traitants en systématisant cette approche par les risques. Nul besoin de vanter les mérites du dispositif qui a défrayé la chroniques ces dernières années. Sa force de frappe est d'autant décuplée qu'il s'applique de plein droit sans effet d'interprétation dans les législations nationales à la différence de la Directive NIS qui nécessite un travail de transposition administrative.

A l'instar de l'ANSSI, nous présentons également nos meilleurs vœux pour aboutir à une démarche d'étude des risques visant à mettre sous contrôle les tiers intervenant sur la chaine de valeurs des OSE.

Nous pressentons qu'il s'agira de la thématique phare de l'année 2021.