Et si l'ENISA devenait le vrai NIST Européen ?

Guillaume COLLARD
Associé fondateur
CSB.SCHOOL

Le National Institute of Standards and Technology (NIST), ce nom ne vous dit sûrement rien si vous ne travaillez pas dans le domaine de la recherche, de l'industrie ou des technologies. Mais si, à l'inverse, vous évoluez dans un de ces mondes et notamment celui de la Cybersécurité, ce nom doit vous être extrêmement familier.

Le NIST dans le monde de l'informatique et de l'informatique industrielle, qu'est-ce que c'est ?

Une agence d'Etat américaine rapportant au Département du Commerce qui développe, entre autres, des normes de concert avec l'industrie du secteur des Technologies, de l'Information et des Communications (TIC). Ces normes ayant deux objectifs principaux :
- donner un support compréhensible de règles permettant de bien concevoir, déployer et gérer ses systèmes avec une vision à la fois "technologie" et "process" ;
- apporter un support documentaire pour soutenir efficacement les réglementations fédérales ou sectorielles des Etats-Unis.

Les Etats-Unis ont donc une institution qui soutient les organisations dans leur démarche de conformité réglementaire tout en préservant l'intérêt des Etats-Unis et de son économie.

Qu'en est-il de l'Europe ?

L'équivalent Européen de NIST est l'ENISA (The European Union Agency for Cybersecurity). Cette agence européenne constitue l'organe central pour tous les sujets Cyber de l'Union Européenne en portant par exemple le Cybersecurity Act de 2019 qui lui confère sa capacité d'action. Sur papier, l'ENISA est officiellement le NIST Européen.

L'ENISA émet donc des publications permettant d'accompagner les Etats membres et les organisations dans leur démarche de conformité et de sécurisation de leur environnement numérique.

Pour autant, à date, le NIST fait office de référence au niveau Européen devant l'ENISA.
Mais pourquoi ?

Pour comprendre cela, prenons un exemple concret et intéressons-nous au sujet de la cryptographie. La cryptographie est un sujet intéressant car il est souvent au cœur de sujets extrêmement sensibles comme les réglementations portant sur la sécurisation des données militaires, doubles usages, personnelles, de santé, financière etc. Il est souvent utilisé comme un argument (marketing) permettant de rassurer les organisations et les États sur la sécurité d'un système et des données qui lui sont associés.

Le NIST Special Publication 800-175A [1] est une publication qui présente les Standards Cryptographiques à utiliser par les organisations fédérales américaines et sur base du "volontariat" pour les autres organisations. Le mot volontariat est à pondérer sachant que la section 2 du Standard présente l'ensemble des lois américaines qui sont impactées par cette publication et donc qui obligent, *de facto*, à suivre ces règles. Cette publication explique de manière détaillée les mesures de sécurité applicables dans le domaine de la cryptographie, les techniques à utiliser, etc. Elle est soutenue par un programme de validation des modules cryptographique (CMVP) [2] et un programme de validation des algorithmes cryptographiques (CAVP) [3]. Le CAVP est lui-même soutenu par une publication, la série 140 du Federal Information Processing Standards, plus connue sous le nom FIPS 140. Le processus est simple, chaque organisation peut soumettre un module de chiffrement et / ou un algorithme de chiffrement qui sera analysé par le NIST (dont le code source et les commentaires du code source expliquant en détail son fonctionnement) afin de savoir s'il répond ou non aux exigences de sécurité imposées par les Etats-Unis. Si c'est le cas, l'algorithme et ou le module est référencé dans la base de données accessibles ici et devient ou peut devenir FIPS approved et NIST recommended. Ceci permettant aux organisations impactées par une réglementation les obligeant à utiliser une technologie cryptographique certifiée de pouvoir choisir librement dans la base de données.

Dans le cas des algorithmes de chiffrement symétrique, le NIST organise des concours appelés Advanced Encryption Standard (AES) permettant de sélectionner l'algorithme qui fera référence dans cette catégorie. L'algorithme gagnant récupère d'ailleurs le nom du concours. Exemple : l'AES très connu dans le monde cryptographique est un algorithme nommé Rijndael qui a remporté le concours de 2001 et qui porte désormais le nom du concours, comme pour effacer son passé et rappeler au monde que cet algorithme est désormais américain.

NIST travaille également de concert avec la NSA (National Security Agency) pour émettre des fonctions de hachage robustes connues sous le nom de Secure Hash Function (SHA). Le NIST organise également des concours pour les Signatures Digitales (RSA), etc. Par le biais de ce programme, le NIST contrôle le monde cryptographique en dictant quels seront les algorithmes et modules qui régneront dans le monde Cyber. En effet, quand bien même un algorithme soit performant, tant qu'il ne sera pas reconnu par NIST, très peu d'organisations prendront le risque de l'utiliser, ceci afin d'éviter les lourdes sanctions liées à un défaut de conformité.

A ce jour, il n'existe aucun programme de ce genre en Europe.

Si nous nous concentrons sur les publications de l'ENISA, ces dernières mettent l'accent sur les techniques de chiffrement, leurs forces et faiblesses en évoquant par ailleurs AES et SHA de façon théorique à l'image d'un module scolaire. Mais, à aucun moment, ils ne mettent l'accent sur le caractère stratégique de détenir le pouvoir de sélection des algorithmes à appliquer au sein de l'Union Européenne.

Attention, ne nous méprenons pas sur les intentions de ce papier.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf

[2] https://csrc.nist.gov/projects/cryptographic-module-validation-program

[3] https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program#:~:text=The%20NIST%20Cryptographic%20Algorithm%20Validation,prerequisite%20of%20cryptographic%20module%20validation.

En aucun cas nous remettons en cause la qualité de l'AES (Rijndael), de SHA 3 ou encore RSA. Nous attirons l'attention sur le fait qu'aucune technologie européenne ne peut ou ne pourra exister de manière "sérieuse" au niveau International / Européen sans le fameux tampon du NIST et donc, par conséquent, des Etats-Unis. Le dernier exemple en date est l'algorithme Falcon développé par Thalès pour répondre aux enjeux du post quantique qui vient d'être sélectionné par le NIST comme standard cryptographique post-quantique pour les signatures digitales. Un succès français qui n'est un succès que parce que le NIST a donné son accord. Pas l'ENISA, mais bien le NIST. Est-ce que cet algorithme répondra aux enjeux de sécurité des Européens ? Nous n'en savons rien car à l'inverse du NIST, nous ne testerons pas et nous suivrons les recommandations américaines les yeux fermés.

A ce jour, l'AES est considéré par la communauté cyber comme un algorithme fiable et sécurisé entre autres car les Etats-Unis l'autorisent toujours. Pour autant en 2003, le gouvernement américain avait annoncé : "L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ». Le niveau « TOP SECRET » nécessite des clés de 192 ou 256 bits. L'implémentation de l'AES dans des produits destinés à la protection des systèmes et/ou documents liés à la sécurité nationale doit faire l'objet d'une analyse et d'une certification par la NSA avant leur acquisition et leur utilisation".
Rappelons que la NSA travaille à détecter des faiblesses dans les algorithmes de chiffrement et qu'elle a accès aux codes sources ainsi qu'aux commentaires. Lorsqu'elle en détecte, elle choisit généralement de ne pas les communiquer mais demande aux institutions américaines traitant des données hautement confidentielles de ne pas les utiliser ou alors de faire valider leur usage. Il y avait eu des précédents entre autres sur l'algorithme de chiffrement DES. En suivant aveuglément le NIST, les Européens font le choix de décentraliser leur capacité de contrôle et de maîtrise de la protection de leur données et éventuellement de leurs données stratégiques. Si jamais la NSA avait trouvé un moyen de déchiffrer un message protégé en AES via une faiblesse de ce dernier, nous n'en serions rien pendant un certain temps jusqu'à un énième scandale PRISM et Upstream Collection.

Cette posture ne serait pas gênante si les dernières réglementations européennes ne cherchaient pas à effectuer une forme de protectionnisme européen et si le débat public et politique n'était pas un concentré de souverainisme.

Pour conclure, toutes ces volontés ne pourront être couronnées de succès tant que l'Europe ne possédera pas une organisation à la hauteur du NIST.

Il existe une dichotomie de posture en Europe. Certains pays ont d'ailleurs fait un choix stratégique pour répondre à cette problématique comme la Chine qui s'arme et se structure comme les Etats-Unis avec le National Information Security Standardization Technical Committee (TC260) afin de déterminer quelles sont les mesures de sécurité les plus pertinentes pour répondre à ses enjeux stratégiques[4]. Le TC260 a approuvé en 2020 huit standards de Cybersécurité.

Pour revenir à notre exemple, vous vous en douterez en matière de chiffrement, les recommandations chinoises ne sont pas obligatoirement les mêmes que celles des Américains. Ce qui inquiète fortement ces derniers, surtout pour tout ce qui concerne le domaine des nouvelles technologies (NTIC) et en particulier les télécommunications (5G et 6G). Ceci

[4]Chinese Central Strategy National Security Publication http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm

les a d'ailleurs amenés à diligenter l'étude suivante : "L'article 9414 de la loi sur l'autorisation de la défense nationale (NDAA) de 2021 qui ordonne au NIST de conclure un accord avec une entité appropriée pour mener une étude et fournir des recommandations concernant l'effet des politiques de la République Populaire de Chine (RPC) et la coordination entre les entités industrielles au sein de la RPC sur les organismes internationaux engagés dans le développement et l'établissement de normes internationales pour les technologies émergentes".[5]

Force est de constater que l'ENISA et l'Europe ne représentent pas à ce jour une source d'inquiétude pour les Etats-Unis ou la Chine compte tenu de l'approche et de la gouvernance adoptée sur le sujet.

[5]https://www.federalregister.gov/documents/2021/11/04/2021-24090/study-on-peoples-republic-of-china-prc-policies-and-influence-in-the-development-of-international