CESIN

AGENCE DE NOTATION CYBER

POSITION PAPER

Juin 2023

Message du Conseil d 'Administration

Juin 2023

Intérêt d'un document "Position CESIN" sur les Agences de Notation Cyber

Un précédent … la notation financière

Au lendemain de la crise financière de 2008, des entreprises bien notées, ont déposé le bilan et le monde s'est aperçu de la fragilité du système de notation financière. Pourtant, ce système fait encore référence car il répond à un besoin de simplification, d'homogénéisation et de neutralité supposée de l'évaluation, dans la mesure où cette évaluation est donnée par un tiers. Le rapport du Sénat de 18 juin 2012(1) décrit le rôle de ces agences comme celui de tiers de confiance visant à réduire l'incertitude des risques pris par les assurances, les banques et les investisseurs.

En dépit de la crise, des constantes subsistent toutefois :

- les systèmes de notation comme mode de régulation du risque ;
- l'acceptation de « tiers de confiance privés » comme régulateurs.

Parmi les problèmes mis en évidence par un rapport du Sénat(1) il y a : la **transparence** ; la **délocalisation du droit** ; la **pertinence des analyses produites** ; la **distorsion de notation** ; **un modèle économique émetteur payeur** qui induit un doute sur le conflit d'intérêts. Ces problèmes connus de tous peuvent être exploités dans le cadre d'action de déstabilisation à l'encontre d'organismes et/ou de dévalorisation de leurs actifs économiques (prédation). Pourtant nous sous-traitons toujours ce rôle de régulateur à des organismes privés, battant pavillon étranger (généralement américain ; plus de 94% du marché), sans réelle alternative européenne.

Cet engouement ne se limite plus désormais au domaine financier. Toutes les activités ayant un rôle dans le circuit économique peuvent être notées. **Le domaine de la Cybersécurité n'y échappe pas et l'on assiste depuis quelques années, outre-Atlantique, à l'émergence d'une offre privée non-régulée qui se déploie désormais en Europe.**

A l'image de la notation financière et à l'heure où l'importance accordée à la Cybersécurité ne cesse de se développer, les pratiques de notation cyber devraient peu-à-peu intégrer les contrats, à l'achat comme à la vente. Les notes attribuées par des agences, individuellement ou au sein de « panier de notes » vont prendre place dans les contrats d'assurance, de sous-traitance (notamment référencement) et de cessions d'actifs (Fusion et Acquisition).

Nous proposons d'aborder dans ce « Position Paper » les points suivants

1. LES DIVERS USAGES DE LA NOTATION CYBER CONSTATÉS DANS NOTRE COMMUNAUTÉ … ET DES APPORTS IDENTIFIÉS
2. DES AXES D'AMÉLIORATION IDENTIFIÉS
3. PLUSIEURS CONSIDÉRATIONS À PRENDRE EN COMPTE
4. DES RECOMMANDATIONS ÉMISES PAR LE CESIN

Il s'agit désormais de créer au sein de la filière Cybersécurité, avec les contributions des adhérents du CESIN, les conditions pour anticiper l'évolution des risques Cyber et contribuer à harmoniser et fiabiliser les pratiques des Agences de notation Cyber aux niveaux français et européen.

ILS L'ONT DIT

« IL N'EXISTE AUCUNE GARANTIE D'INDÉPENDANCE, AUCUN CONSENSUS SUR LA VÉRITABLE VALEUR DES NOTATIONS DE RISQUE CYBER PUBLIÉES PAR L'OLIGOPOLE DES AGENCES AMÉRICAINES. »
Arnaud MARTIN et Didier GRAS
CYBERSECURITE. Vigile de notre autonomie stratégique. Juin 2022. Digital New Deal

Ce document intitulé « Position Paper » est destiné aux adhérents du CESIN. Il leur donne la position du CESIN sur des sujets transverses, sociétaux et stratégiques au sein de la Filière Cyber. Par ailleurs, ce document a vocation à être mis à jour de façon régulière au regard de l'actualité. Contacts : alain.bouille@cesin.fr , gestion.cesin@cesin.fr

(1) Audition devant la mission commune d'information du Sénat le 9 mai 2012.
Source : http://www.senat.fr/rap/r11-598-1/r11-598-11.pdf

POSITION CESIN

AGENCE DE NOTATION CYBER

1. LES DIVERS USAGES DE LA NOTATION CYBER CONSTATÉS DANS NOTRE COMMUNAUTÉ …

Contexte : Le CESIN questionne toutes les semaines l'ensemble de sa communauté sur une thématique donnée. Cela permet d'avoir une mesure instantanée et sans aucun filtre marketing sur cette thématique, afin d'établir un état des lieux et/ou se benchmarker.

Les pratiques de notation cyber (cyber rating) se développent que ce soit dans le cadre de contrats d'assurance, de contrats de sous-traitance ou tout simplement pour mesurer son niveau d'exposition publique.

Comment utilisez-vous ce type de services ?

Source : Question de la semaine n°105 – Avril 2023

55% des répondants utilisent les services des agences de notation pour des besoins divers.

Dans vos entreprises vous êtes (plusieurs réponses étaient possibles) :

- **45%** à ne pas utiliser les services des agences de notation
- **39%** à utiliser ces services comme l'un des moyens de surveiller votre exposition publique et détecter vos défauts de sécurité pour y remédier au plus tôt
- **34%** à utiliser ces services pour des questions d'image, de benchmark et de réputation de votre entreprise vis-à-vis de tiers
- **23%** à utiliser ces services dans le cadre de la négociation de votre police de cyber assurance
- **17%** à utiliser ces services pour faire réagir les dirigeants de votre entreprise
- **16%** à utiliser ces services pour mesurer le niveau de maturité de toute ou partie de vos tiers (fournisseurs, partenaires)
- **7%** à avoir d'autres usages de ces services

*Répartition sur les **179** répondants par taille d'entreprise : 53% (grandes entreprises), 35% (ETI), 12% (TPE/PME).*

Toute société peut se permettre d'établir à tout moment, sans informer systématiquement l'organisme visé, sur un périmètre non vérifié, une note Cyber. Cette note est commercialisée, communiquée à des Tiers (partenaires, concurrents, autorités, …) et dans certains cas rendue publique.

… ET LES APPORTS IDENTIFIÉS

- Un accélérateur **pour la maitrise de sa surface exposée** (empreinte numérique). Cette surface est de plus en plus importante à prendre en compte de manière exhaustive et il faut la réévaluer en continu.
- Une incitation à une **plus grande réactivité** des équipes internes pour la mise à jour de correctifs lorsque des failles critiques sont détectées, même s'il faut rester vigilant devant les (longues) listes de failles mineures remontées par le système de notation, vis-à-vis desquelles les équipes peuvent se désengager au profit de sujets de sécurité interne jugés bien plus prioritaires.
- Une **appréciation de la simplicité d'un indicateur composite Cyber** sous la forme d'une note, sous forme de lettre ou de chiffre.
- Un **soutien renforcé de la direction de l'organisme** qui, ne souhaitant pas à avoir à se justifier d'une note faible, va globalement renforcer les moyens alloués à la cyber.
- Une capacité de **vérifier la bonne configuration de ses produits installés** chez des tiers.
- Une **approche compétitive « gamifiée » qui crée de l'émulation entre filiales d'un organismes ou entre cet organisme et ses concurrents.**
- Une possibilité de **suivre les variations** de ses tiers et filiales et d'alerter.
- Un **indicateur, même partiel,** sur un tiers, et lui faire savoir que vous le suivez.
- Un message de **bonne gestion de votre surface exposée** aux cyber assureurs, pour les rassurer, et aux hackers, pour tenter de les dissuader d'essayer, surtout si la note reste stable.

Une notation complète devrait combiner une étude externe, un questionnaire SMSI et des KPI techniques incluant le périmètre interne. Les questionnaires et KPI doivent eux aussi être limités et standardisés afin d'économiser les ressources des sociétés auditées.

L'idée d'un pilotage à partir d'une note Cyber composite est attrayante.
Une automatisation des mesures par un tiers qui évalue des progrès et fournit un benchmarking (selon le secteur d'activités, la taille de l'organisme) peut apporter un intérêt mais il reste des points d'amélioration importants pour en faire un véritable outil contribuant au pilotage de la cyber, pour les adhérents du CESIN.

CESIN

2. DES AXES D'AMÉLIORATION IDENTIFIÉS

Le droit d'accéder à l'exhaustivité de ce qui est associé à la note, l'obligation de réactivité de mise à jour des données par l'agence, la capacité à contester les assignations sur le périmètre d'une organisation et ce qui serait rendu visible

- Les notations actuelles représentent une vision partielle du niveau de sécurité de l'organisme, la part dite externe ou publique en partant du postulat qu'il s'agit d'un échantillon représentatif de la sécurité globale. Or une entreprise qui aurait, par exemple, de très mauvaises pratiques sur ses réseaux et systèmes internes ainsi que sur sa gestion des identités et des accès, pourrait obtenir une très bonne note juste en soignant sa surface exposée. A contrario, une entreprise qui gèrerait ses risques efficacement et refuserait de « jouer la note », pourrait temporiser la correction de certaines vulnérabilités mineures externes pour se concentrer sur le traitement de risques et vulnérabilités majeurs liés à des actifs non visibles de l'agence de notation. L'agence ne peut observer qu'un seul axe de la sécurité et cette approche n'est pas suffisante. Or il n'existe pas encore, à ce jour, de méthode et de référentiels d'évaluation qui fassent consensus, qui soient réalistes dans leur mise en œuvre à l'échelle, et incontestées par l'écosystème cyber.
- Ces notes et leurs fluctuations ne sont qu'un faisceau d'indices sur le niveau de sécurité, d'autant qu'une organisation qui n'aura pas sollicité ce service ne pourra pas défendre le choix managérial qu'il a fait, en terme de gestion des risques. De plus, une bonne note n'est pas la certitude d'une posture cyber mature, notamment si l'empreinte externe est faible. De même, une note moyenne ne représente pas une mauvaise posture dans le cas, par exemple, où l'entreprise fait de l'hébergement de compte de tiers.
- La pertinence des analyses de l'exposition publique dépend de la qualité de la cartographie associée à l'organisation évaluée, cartographie qui dépend de l'interprétation de l'agence et de la volonté du noté d'y apporter les corrections nécessaires. Souvent, le seul fait d'être noté, encourage, voire oblige l'entreprise à fiabiliser la cartographie de ses actifs externes. Ces données d'entreprise devraient faire l'objet d'un droit de portabilité afin de faciliter la notation par différentes agences.
- La profondeur et le niveau de qualité d'analyse des notations varient en fonction des agences : elles peuvent ou non croiser plusieurs sources d'informations (CTI – Cyber Threat Intelligence, contrôles, …) et les coupler à des analyses humaines. La question de la compétence des analystes peut alors se poser dans un contexte de marché des talents cyber fortement concurrentiel et de jeunesse de la discipline.

L'amélioration de la transparence des algorithmes et des pondérations, et la clarification des méthodes de collecte

Les principes, méthodes et pondérations menant à la publication d'une note restent propriétaires, donc différents entre les agences de notation. Il n'y a pas, à date, de norme ou de consensus pour définir la méthodologie attenante à une note ou une évaluation. Chaque agence de notation cyber propose aujourd'hui le résultat de son algorithme « maison » et l'analyse de ses propres experts. Chacune des agences pourrait prétendre à ce que ses méthodes deviennent un standard de fait qui finirait par s'imposer à tous. La jeunesse de la pratique entraîne aussi quelques dérives qu'il conviendrait de cadrer d'autant qu'elles imposent parfois des arbitrages desservant l'intégrité recherchée par les experts.

L'établissement d'un référentiel partagé au sein de la filière pourrait supporter :

- La proposition d'offres de notations claires et transparentes.
- La mise en place d'une garantie de la compétence des analystes et de la cohérence des interprétations en cas de litige, notamment d'ordre contractuel.
- La reproductibilité des analyses et la clarification de la méthode de calcul des notes (barèmes et pondération).
- L'application du principe d'amélioration continue.

Enfin, l'établissement d'une norme de mesure et de présentation permettrait de normaliser la communication sur le marché mais aussi auprès de Comités Exécutifs et de Conseils d'Administration qui mésinterprètent parfois les notations si celles-ci sont présentées comme l'unique levier de la mesure de performance cybersécurité, ce qui est loin d'être le cas.

La distorsion de notation

- L'empreinte numérique établie a priori par les agences comporte un taux d'erreur non négligeable en ce qui concerne l'assignation des actifs à l'organisme noté, et c'est dans cette portion mal attribuée que réside le plus fort taux d'anomalies détectées. Si L'organisme souscrit au service, il peut faire rectifier son périmètre assigné. Compte tenu de la relation existante avec les entreprises clientes et de la qualité de l'empreinte associée, la qualité de la notation varie sensiblement en fonction du statut payeur ou non-payeur.
- A contrario, l'absence de maitrise de l'empreinte par l'entreprise évaluée ouvre la possibilité de « manipulation » des scores, voulue ou non, au travers de bais d'interprétation et ou d'effet de cascade.

La préservation d'une certaine autonomie par une ségrégation des prestations

- Il apparaît que certaines agences de notation font de la vente croisée avec du service pour l'aider à améliorer la notation selon un algorithme qu'elle seule connaît. L'entreprise pourrait donc être liée à l'agence pour obtenir des résultats acceptables sur sa notation. Il semble important d'éviter les conflits d'intérêts des agences. A ce titre, rappelons que la vente de services additionnels de certains organismes attribuant des notes a été interdit pour les agences financières.

A ce stade, la façon, dont ces notes sont conçues, délivrées et communiquées, nécessite de les prendre avec une certaine précaution. Pour donner de la pertinence aux notations, cela nécessite des actions de vérification du RSSI et d'adaptation au contexte des entreprises et aux plans de gestion des risques en place.

3. PLUSIEURS CONSIDÉRATIONS À PRENDRE EN COMPTE

Permettre une prise de conscience du modèle économique et de ses limites, et ouvrir sur des enjeux d'intelligence économique

- L'agence de notation est d'abord payée par l'organisme voulant connaître sa note et l'améliorer.
- L'agence de notation bénéficie ensuite des ressources engagées par l'entreprise pour fiabiliser ses données. L'agence ne peut pas établir une empreinte numérique totalement fiable et traite en général les assets les plus faciles à identifier et à assigner à l'organisme. L'entreprise doit alors faire des dépenses complémentaires pour traiter et corriger la cartographie retenue, part la plus difficile et la plus coûteuse à réaliser. L'organisme finance ainsi la fiabilisation des données, qui revient ensuite à l'agence.
- L'agence de notation revend éventuellement les données de notation, sur la base de ses analyses, fiabilisées par l'organisme, à des assureurs, des concurrents et/ou partenaires qui veulent prendre connaissance de la note de l'organisme.

Si la note peut aider à se donner une idée du niveau d'hygiène de son périmètre et remédier à certaines vulnérabilités vu de l'extérieur, elle peut conduire à certaines déviances. L'approche marketing (en opposition à une approche centrée sur les risques) peut inciter le Responsable Cyber à chercher une bonne note pour la bonne note afin de payer moins d'assurance, de gagner des contrats, de gagner l'attention de son Comité Exécutif. L'approche exclusive sur la base d'une notation pourrait aussi empêcher certaines entreprises de pouvoir mener des évaluations complètes de tiers, les tiers s'appuyant sur leur notation et refusant de répondre à des questions et audits complémentaires.

Toute entreprise peut faire l'objet d'une notation qu'elle le désire ou non. Sans autorisation explicite, l'usage d'outils techniques ayant accès au système d'information d'un organisme pourrait tomber dans le périmètre d'application des textes juridiques. Ainsi pour disposer des notes demandées par les tiers (clients, assureurs ou investisseurs), la contractualisation avec une ou plusieurs agences pourrait devenir une obligation.

L'absence d'offre de notation européenne, avec en parallèle l'émergence de critères américains dans les contrats nationaux ou européens, constituent une vulnérabilité supplémentaire en matière d'extra-territorialité. Le stockage des données (cartographie des assets, vulnérabilités et actifs critiques tiers) hors Union Européenne les exposent potentiellement à une intelligence compétitive étrangère.

Une empreinte numérique d'une entreprise (ou « surface d'attaque ») établissant et consolidant les @IP, les noms de domaines, les partenaires, les sites Web a une valeur indéniable lorsqu'elle est vérifiée et validée par l'entreprise visée. L'identification de l'écosystème (prestataires) de cette entreprise qui vient compléter l'empreinte numérique devient une information sensible et ne peut être manipulée sans contrainte.

4. DES RECOMMANDATIONS ÉMISES PAR LE CESIN

A la lumière de ce qui a été exposé précédemment dans ce Position Paper, le CESIN souhaite :

- Obtenir plus de transparence des méthodes et des algorithmes utilisés par les agences de notation pour la découverte des assets et l'attribution de notes avec les coefficients de pondération.
- Favoriser le développement d'agences de notation européennes.
- Réguler le mandat des agences en leur interdisant la vente en parallèle de prestations visant à aider les organismes à améliorer les scores obtenus.
- Contribuer à la production d'un dispositif d'évaluation des organismes au plan cyber, sur plusieurs axes fondamentaux, afin que la mise en œuvre soit réaliste, transparente, reproductible et efficace. Ce dispositif :
  - Devrait être construit en consultant les différents acteurs actuels de l'écosystème cyber
  - Peut inclure, entre autres et comme l'un des critères d'évaluation, l'exposition publique que traite les agences de notation actuelles.
  - Doit établir des résultats à partir de plusieurs sources d'évaluation, afin d'éviter tout risque lié aux intérêts d'une agence unique.

SOURCES ET POUR ALLER PLUS LOIN …

- **Livre blanc – Cyber rating**. Source Forum des Compétences 2019
Livre blanc – Cyber rating (forum-des-competences.org)

- **Cyber Risk Index et Cyber Notations**.
Lundi de la Cybersécurité. ARCSI et Université de Paris. Pierre-Luc REFALO. VP Capgemini Group Cybersecurity. Octobre 2021

- **Livre blanc Cybersécurité.** Vigile de notre autonomie stratégique.
The Digital New Deal. Juin 2022. - Cybersecurite-DigitalNewDeal-Mai2022.pdf (thedigitalnewdeal.org)