Information Security

SECURITY RATING

provadys

AVIS D'EXPERT
Security Rating, opportunité ou malédiction ?

Auteur :
Julien Steunou, Lead SOC Provadys

De gré ou de force et de façon plus ou moins consciente, la plupart des entreprises sont confrontées au sujet du security rating qui mesure leurs performances cyber sécurité sur le modèle de ce qui existe depuis des décennies pour les notations financières standardisées portées par des sociétés comme Moody's, Standard & Poor's ou Fitch Rating.

Le principe commun à toutes les solutions de security rating est de produire une note représentant la performance et la maturité cyber sécurité d'une organisation par une évaluation automatisée, continue et reproductible sur la base de données observables publiquement.

Développées depuis plusieurs années dans le monde anglo-saxon, ces solutions sont de plus en plus utilisées en France par des assureurs, investisseurs et organismes financiers, mais également par les entreprises elles-mêmes pour évaluer les risques cyber sécurité de leurs prospects, clients, fournisseurs et partenaires et éclairer des décisions qui ont des impacts directs dans le business de tous ces acteurs : montant des primes d'assurance, évaluation des propositions dans l'attribution de marchés, valorisation lors d'opérations de fusion / acquisition…

Un nombre croissant d'entreprises de toute taille ont bien identifié l'importance de leur propre security rating, ou les opportunités qu'elles pouvaient avoir d'utiliser ces systèmes pour évaluer leurs sous-traitants et gérer les risques liés à leur écosystème. Reste que la majorité d'entre elles subissent les conséquences d'une mauvaise notation comme une malédiction sans le savoir.

Comment fonctionne un security rating ?

C'est la combinaison de trois activités :

1. Une cartographie des actifs techniques publics de l'entreprise pour associer à une entreprise un ensemble d'IP publiques, noms de domaines, sites web…
2. Une collecte de données publiques sur ces actifs techniques pour relever des traces de compromission ou activité malveillante (ex : une IP de l'entreprise connue comme étant un nœud de sortie TOR / participant à un botnet ou un site web identifié comme diffusant/propageant du malware) et réaliser des tests simples pour évaluer la rigueur des configurations (ex : conformité de la configuration SSL/TLS d'un site web à l'état de l'art, utilisation de SPF sur le domaine de messagerie…).
3. Une analyse par un algorithme de notation qui produit une note combinant les éléments négatifs et positifs associés aux actifs techniques attribués à une société avec certaines pondérations, des subtilités comme la réactivité constatée à régler un problème ou l'historique d'incidents de sécurité connus de l'entreprise (moins évident à exploiter en France qu'aux USA, mais les réglementations mettant une pression croissante sur les obligations de notification, il est probable que des bases de données se constituent chez nous dans les années à venir).

L'algorithme peut produire une note actualisée quotidiennement, donner des tendances et une vue historique pour peu que les données soient disponibles pour recalculer des positions passées. Il faut alors intégrer des mécanismes de soin dans la notation pour que l'impact d'un événement négatif soit progressivement effacé à partir du moment où une remédiation a été observée.

Les agences de notation ayant pour objectif de sortir une notation en continu pour le plus d'entreprises possible, il est évident que tout le process doit rester :

- Totalement automatisé.
- Simple, rapide et sans risque de production pour les actifs techniques testés (ce qui interdit de fait des tests de type scan de vulnérabilité par exemple).
- Sans interaction avec les entreprises évaluées.

Tout le business des agences de notation consiste ensuite à vendre la notation d'une entreprise à qui souhaite l'acheter et au principal intéressé si cela est possible pour un prix variant de quelques milliers à quelques dizaines de milliers d'euros.

Est-ce que les notes sont comparables d'un security rating à l'autre ?

Il n'existe pas à ma connaissance d'étude sérieuse comparant dans le temps le security rating d'un échantillon d'organisations sur plusieurs systèmes. En revanche mes échanges avec différentes entreprises ayant évalué plusieurs solutions (à l'occasion de pilotes ou via la souscription de plusieurs contrats en parallèle), laissent apparaître qu'il y a globalement une convergence des résultats donnés par les différents systèmes (modulo les erreurs de cartographie).

Et pour cause, l'ensemble de la profession exploite les mêmes données externes et un catalogue restreint de tests relativement simples dans l'interprétation de leurs résultats, avec finalement peu d'innovation possible. Des différences existent dans les algorithmes de notation, les pondérations et les mécaniques de soin mais appliqués sur un périmètre suffisamment large, cela ne génère pas d'écarts très significatifs.

Le security rating est-il une escroquerie ?

J'ai été personnellement confronté pour la 1ère fois au sujet du security rating en 2016, quand le management d'une grande entreprise pour laquelle je travaillais avait été informé d'une notation défavorable et souhaitait que le CSIR se saisisse du sujet. Je me souviens que ma réaction initiale en approchant le sujet a été proche de « mais quel idiot peut penser qu'une note calculée depuis des tests externes simplistes est représentative de la sécurité d'une entreprise ? ».

C'est probablement la 1ère réaction qu'ont l'immense majorité des professionnels de la cyber sécurité quand ils approchent le sujet, avec un rejet d'autant plus fort qu'ils sont dans l'expertise technique ou dans des activités de sécurité offensive !

Et force est de constater que la majorité des systèmes de security rating prêtent un large flanc à la critique.

Les extrapolations « sauvages »

La majorité des tests réalisés et observables pris en compte sont pertinents et l'interprétation qui en est faite dans la notation tout à fait valide. En revanche la majorité des solutions de security rating inclut un petit nombre de contrôles réalisant des extrapolations hasardeuses à partir des mesures effectuées. Ce sont ces extrapolations, que j'appellerais « sauvages », qui concentrent aujourd'hui les critiques.

Pour bien comprendre la raison de ces extrapolations sauvages, mettons-nous un instant à la place d'une agence de notation voulant vendre sa solution de security rating à de grands assureurs souhaitant développer leurs polices d'assurance cyber. Les assureurs détaillent les sinistres auxquels ils sont confrontés et il en ressort que les ransomwares sont dans le top 3 des incidents de sécurité. Pour signer son contrat, l'agence comprend qu'il est essentiel que sa solution prenne en compte la performance de l'entreprise face au risque posé par les ransomwares.

L'équipe de R&D sollicitée par le commerce de l'agence de notation se pose alors la question suivante : « comment évaluer la performance d'une entreprise face aux risques de ransomware ? » Tout professionnel de la sécurité sait que la performance d'une organisation face au risque de ransomware dépend de l'efficacité de multiples mesures de sécurité : le filtrage sur la messagerie et la navigation web, la gestion des vulnérabilités sur les postes de travail, les contrôles sur les serveurs de fichier, la segmentation du réseau, l'efficacité du plan de sauvegarde… Autant de mesures de sécurité internes qui ne laissent pas de traces observables en externe.

Mais le problème d'une agence de notation ayant la prétention de servir des notes actualisées quotidiennement pour toutes les entreprises du monde est qu'elle ne peut sortir de ses contraintes d'automatisation et de non-interaction avec les entreprises évaluées. Elle ne peut donc pas aller chercher d'information sur ces mesures de sécurité internes qui l'obligerait à poser des questions et à interpréter des réponses complexes. Il faut alors trouver une idée ne remettant pas en cause le modèle initial permettant d'exploiter de la donnée externe disponible.

La R&D trouve alors sous la pression une idée : « si nous collections des informations via des sinkholes ou en achetant des données à des sites à fort trafic et/ou opérateurs, nous pourrions avoir une table associant tous les user-agents (chaîne de caractère envoyée par le navigateur au serveur web dans l'entête HTTP et donnant le nom de l'application, la version, le système d'exploitation, la langue…) vus récemment sur toutes les IP publiques. A partir de cette table, nous pourrons déduire si les versions de navigateur et des systèmes d'exploitation sont récentes, et par un raccourci étonnant en déduire une note sur la sécurité interne globale de l'entreprise ! »

Voilà comment naissent des extrapolations sauvages dans des systèmes de security rating qui alimentent les réserves, voire l'hostilité de beaucoup de professionnels de la sécurité qui voient bien les ficelles et savent que la cyber sécurité n'est pas aussi simple. Mais les principaux consommateurs de ces notes n'étant pas des experts cyber, le marketing de certaines agences fait des merveilles.

Les incohérences de cartographie des actifs techniques

Pour une agence de notation, la cartographie permettant d'associer en temps réel à toutes les entreprises les actifs techniques externes qui doivent être pris en compte dans leur security rating est un défi autrement plus grand que la collecte et l'interprétation des données concernant ces actifs. Elle nécessite des moyens techniques et des armées d'analystes pour assurer la cohérence et la qualité des associations.

Les challenges sont nombreux :

- Trouver des sources d'informations exploitables, en commençant par des sources IT comme les différents registres publics de type Whois, RIPE (à noter que le RGPD a limité les capacités de pivot sur les informations Whois) et les bases de données sur les sociétés.
- Gérer les actifs techniques qui sont mutualisés : par exemple sur une IP publique d'un hébergeur, savoir attribuer ce qui relève du security rating de l'hébergeur même ou des multiples clients qui hébergent des services sur l'IP en question.
- Tracer les changements de propriété pour ne pas impacter le security rating d'une entreprise qui exploite des actifs dont le précédent propriétaire était peu regardant sur la sécurité.

Cartographier des grands comptes demande de réussir à gérer des SI tentaculaires et la complexité des filiales, cartographier de petites entreprises exige de trouver des informations sur des organisations ayant massivement recours à des infrastructures mutualisées, voire des connexions grand public.

La tâche est à l'évidence titanesque et source de nombreuses erreurs d'association, au bénéfice comme au détriment des entreprises évaluées. Cela donne parfois des situations ubuesques où une entreprise découvre que sa notation par une des agences est nulle en raison de la prise en compte d'actifs techniques d'une société étrangère dont le nom est proche du sien. Beaucoup d'entreprises ayant souscrit des contrats avec des agences de notation l'ont bien compris et jouent au chat et à la souris avec le système de cartographie, les notifiant d'erreurs d'association préjudiciables, mais se gardant bien de leur signaler un pan du système d'information non cartographié.

Le problème est que, sauf à souscrire des contrats avec toutes les agences de notation, il est impossible pour une entreprise de suivre comment elle est cartographiée et de repérer les erreurs !

Reste que ces systèmes de cartographie en temps réel produisent en eux-mêmes une valeur que certaines agences de notation exploitent intelligemment : la capacité d'identifier l'ensemble des entreprises partageant un même hébergeur ou opérateur qui devient un SPOF (single point of failure) pour tout un écosystème. Cela intéresse un assureur pour identifier des risques systémiques : si un grand nombre de ses clients utilisent les services d'un même hébergeur, une défaillance de ce dernier générera un énorme sinistre pour tous ses clients. L'intérêt est le même pour une entreprise dans l'évaluation des risques de sa supply chain ou d'un investisseur par rapport à son portefeuille.

Le casse-tête de la prise en compte des exceptions

Certaines entreprises peuvent avoir dans leur stratégie sécurité la mise en place de systèmes volontairement vulnérables (honeypot) ou la pratique de la désinformation (ne serait-ce qu'en modifiant les bannières TCP de certains services). Autant de mesures de sécurité pouvant apparaître à un moteur de security rating comme des manques de rigueur devant être sanctionnés dans l'évaluation.

Remonter ce genre d'information à une agence de security rating avec laquelle l'entreprise a un contrat et la faire prendre en compte en exception dans le rating reste aujourd'hui très compliqué, voire explicitement refusé. Certaines agences peuvent la prendre en compte, mais publieront dans ce cas deux notes : une brute, non retraitée, et une redressée par l'entreprise. Charge à celui qui exploite le security rating de faire son choix entre les deux notes. Traiter ce problème avec toutes les agences avec lesquelles l'entreprise n'a pas de relation commerciale est objectivement quasi impossible pour le moment.

Il est facile de comprendre la difficulté et les coûts de traitement, pour une agence de notation, d'interpréter ce genre de remontée et de démêler le vrai du faux avec des entreprises qui pourraient parfois préférer abuser le système plutôt que de remédier à certains problèmes de sécurité réels.

Pour autant, en dépit de toutes ces faiblesses, peut-on dire que ces systèmes de security rating sont une vaste escroquerie en bande organisée ? Clairement non si nous mettons de côté certains aspects marketing assez regrettables !

La valeur ajoutée réelle du security rating

Victor Hugo écrivait que « la forme, c'est le fond qui remonte à la surface ». Le security rating scrute la forme et en sort de bonnes indications sur le fond. Au cours de mes expériences, j'ai rarement observé d'entreprises gérant très bien leur sécurité interne et présentant une surface d'attaque externe catastrophique. L'inverse en revanche est plus courant avec des entreprises faisant des efforts en externe, mais prenant tous les risques sur leur SI interne. Et effectivement, si j'ai pu parfois être circonspect sur les bonnes notes de certaines entreprises, j'ai rarement été surpris d'une mauvaise notation attribuée à une entreprise dont je connaissais l'envers du décor. Il en découle que pour la prise de décision, un security rating peut parfois conduire à sous-apprécier les risques, mais rarement l'inverse.

La plupart des systèmes de security rating présentent suffisamment de détails sur la notation pour permettre à l'entreprise qui obtient le rapport d'identifier des problèmes de sécurité ou des bonnes pratiques à mettre en place. Pour une petite entreprise, l'apport est réel, car cela permet d'identifier des actions simples dont elle n'avait pas connaissance permettant d'améliorer son security rating, d'améliorer effectivement son niveau de sécurité et de moins passer pour une victime facile. Pour les grandes entreprises qui ont généralement des SOC ou des CSIRT/CERT bien conscients de ce qu'il faudrait faire, cela permet d'avoir un levier supplémentaire pour pousser de bonnes pratiques. Les assureurs ont bien compris l'intérêt d'apporter cette valeur et ce service à leurs clients PME / ETI !

La tension mise par les systèmes de security rating sur certaines bonnes pratiques, ne serait-ce que l'utilisation de SPF/DKIM et DMARC sur les domaines de messagerie, a un effet bénéfique pour toute la communauté. Peut-être même que cela poussera à l'utilisation de DNSSEC, dont l'absence est souvent remontée dans les security rating, même si je suis nettement moins confiant sur ce point !

Comment faire mieux ou différemment ?

Plusieurs entreprises aux USA se sont sérieusement agacées de ces différents problèmes et ont travaillé avec la chambre de commerce US et les agences elles-mêmes pour imposer des bonnes pratiques ainsi qu'une certaine éthique dans le business du security rating.

Les principes sont détaillés dans une publication de la chambre de commerce disponible sur https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings. Les principes posés et la mise en place de tiers de confiance pour aider dans les arbitrages entre entreprises et agences de notation sont d'excellentes initiatives qui mériteraient des équivalents en France.

Les commissaires aux comptes et les experts comptables n'ont pas disparu au profit des agences de notation de crédit. Il en sera de même avec la notation cyber : les tests d'intrusion, les audits techniques et organisationnels, les questionnaires ont toujours un sens. Ils sont les seuls à même de prendre en compte le besoin de sécurité propre à chaque entreprise et d'éclairer sa maturité sur des aspects hors d'atteinte des données externes publiques.

C'est le sens du positionnement du Security Rating développé par Provadys - NetXP : proposer un système d'évaluation associant, dans un système unifié de notation, la simplicité et la rapidité d'une notation automatisée (avec une interprétation honnête des résultats sur le plan sécurité !) et des solutions permettant graduellement de fiabiliser l'évaluation via des vérifications complémentaires : questionnaires, tests techniques avec intervention et interprétation par un expert sécurité, voire audit présentiel.

Passés les premiers grades d'évaluation, cette précision se fait au prix d'une interaction avec l'entreprise évaluée dans un premier temps pour fiabiliser la cartographie de ses actifs, puis réaliser les tests complémentaires. Faire l'impasse sur la cartographie systématique évite une grande partie des problèmes évoqués et permet de proposer des security rating à des prix très compétitifs, mais également de servir des PME / ETI qui par leurs tailles et leur empreinte IT visible sur Internet sont bien souvent sous le radar des agences de notation.

Conclusion

Le security rating est une malédiction pour les entreprises qui restent inconscientes de l'importance de la cyber sécurité et une opportunité pour les autres !

Pour les entreprises négligeant la sécurité de leurs systèmes d'information, il deviendra difficile de le cacher et elles vont subir, parfois sans même comprendre pourquoi, les conséquences de décisions de plus en plus nombreuses de tiers jugeant trop risqué de travailler avec elles.

Pour les autres, passés la première impression et l'agacement largement entretenu par le marketing de certains acteurs, force est de constater que le security rating apporte :

- Un élément de décision appréciable dans la gestion des risques.
- Une présentation simple sinon simpliste des sujets cyber sécurité les rendant accessibles et visibles par des personnes non spécialistes qui n'auraient pas les moyens ou le temps de rentrer dans le détail autrement.
- Une tension positive sur l'application de bonnes pratiques connues, mais souvent négligées.

Pour les professionnels de la sécurité IT, il est désormais incontestable que les security rating rencontrent un succès réel auprès de nombreux décideurs et que la profession est bien obligée de prendre en compte le phénomène pour en tirer le meilleur parti, avec de grands enjeux pour redresser certaines interprétations et avancer sur les remédiations.

L'activité restant jeune, il faut également s'attendre à ce que des approches développant la confiance dans le modèle soient mises en œuvre par de plus en plus d'acteurs et que les autorités publiques ou les régulateurs s'impliquent sur le modèle de la chambre de commerce US.