Assurance Cyber : Prendre le point de vue de l'assureur pour améliorer sa posture cybersécuritaire

Éric VAUTIER
Senior advisor
CyberCercle

De manière assez inattendue, la cyber-assurance suit le fameux *hype cycle* de Gartner, d'ordinaire appliqué aux technologies : après une phase de lancement plutôt réussie ces dernières années, elle semble être au fond du "Gouffre des désillusions", peu de temps après la déclaration de Guillaume Poupard[1] sur le "jeu trouble de certains assureurs", qui, en couvrant le paiement des rançons, encourageraient involontairement les cybercriminels à s'attaquer aux entreprises assurées. Si l'argument fait mouche, ne fournit-il pas aussi aux assureurs un bon prétexte pour revisiter des clauses qui furent peut-être établies légèrement et dont les effets pécuniaires se firent sentir dès l'attaque NotPetya[2] ?

Il nous semble donc intéressant de profiter de cette phase de flottement pour réfléchir à un usage pertinent de la cyber-assurance par les RSSI (Responsable de la Sécurité des Systèmes d'Information), entre le parapluie qu'on ouvre à la première attaque réussie et la police inapplicable tant il y a de clauses d'exclusion, pour établir de vraies relations de confiance et, espérons-le, gravir la "Pente de l'Illumination".

A la lecture de ce qui suit, certains RSSI pourront nous taxer d'angélisme, voire de parti-pris, tant l'argumentaire qui suit penche en faveur des assureurs. Il est évident que la réalité est plus nuancée. Certaines clauses sont encore suffisamment absconses pour que des contentieux comme celui de Merck puissent exister, ce qui jette un voile de défiance sur l'ensemble du sujet. Finalement, les RSSI ne devraient-ils pas adopter résolument les réflexes d'un assureur - imaginer le pire en ne parlant que d'argent - sans pour autant oublier de lire très attentivement les fameuses "petites lignes" du contrat ?

Imaginer le pire

Pour l'entreprise, mener son analyse de risques cyber est finalement assez simple : on liste des événements redoutés et on ne conserve que les plus probables à fort impact. Puis on en tire des plans d'action pluriannuels : pour le Métier, ce sera d'essayer de diminuer l'impact de l'incident ; pour la DSI, ce sera de

[1] Table ronde sur « La cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics » (senat.fr)

[2] NotPetya : Merck bataille avec les assureurs pour 1,3 Md $ d'indemnisation - Le Monde Informatique

mettre en œuvre des protections pour baisser la probabilité ; et pour les deux conjointement, de prévoir les plans de continuité et de reprise. Ainsi, on obtient une cartographie des risques résiduels qui satisfait toutes les parties, y compris la Direction Générale de l'entreprise.

L'assureur, de son côté, va se saisir de la cartographie des risques bruts et retenir les scénarios qui vont représenter les coûts les plus importants (pertes d'exploitation, coûts de remise en service, dédommagements des tiers, etc.), puisque, dans le pire des cas, c'est ce montant qu'il faudra verser à son client - sans la franchise.

Cette différence d'approche - minimiser en considérant les contre-mesures versus maximiser en faisant l'hypothèse qu'elles ne fonctionneront pas - crée une incompréhension entre les assureurs et les RSSI qui admettent difficilement que les mesures de protection puissent ne pas être efficaces. Ce côté émotionnel, finalement inattendu dans ce contexte, engendre de facto un biais dans l'évaluation des risques. L'assureur, extérieur au sujet et analysant à froid les éléments, apporte finalement un regard plus réaliste et donc plus pertinent.

Dans cet exercice de définition du contrat de cyber-assurance, il nous apparaît donc préférable de partir des risques bruts et de quantifier les coûts globaux en imaginant le pire.

Ne parler que d'argent

Sans trahir de secrets corporatistes, il existe des biais dans la gestion du risque : l'appréciation des impacts et/ou de la vraisemblance fait l'objet de débats parfois houleux où les arguments ne sont pas toujours de bonne foi : on peut délaisser un domaine historiquement complexe ou à l'inverse privilégier un domaine de sa zone de confort, au détriment finalement du "vrai" risque. En se focalisant sur le coût, on objective le débat - on peut bien sûr ergoter sur le montant final mais, si on l'a sous-estimé, il faudra assumer le jour de l'évaluation des dégâts.

La discussion avec l'assureur peut ainsi aider à estimer un retour sur investissement des mesures qu'on souhaite mettre en œuvre en corrélant une mesure à une diminution de la prime. La franchise quant à elle, utilisée intelligemment, peut équivaloir à un seuil de criticité et aider à la sélection des risques que l'on doit traiter.

Autre avantage de cette approche : sortir de la pensée technologique. Sans trop tomber dans la caricature, la volonté de tout connecter est parfois l'expression d'une forme de facilité managériale : au lieu de fournir deux écrans ou deux téléphones, on va vouloir tout placer sur le même appareil, en faisant souvent cohabiter des environnements de criticités différentes et donc en affaiblissant les mesures de sécurité du plus critique. La meilleure solution est souvent de simplement supprimer ces interconnexions. Ce choix ne sera pas gratuit puisque l'on dégrade probablement l'efficacité opérationnelles des utilisateurs, notion d'ailleurs très difficilement quantifiable.

Les "petites lignes" de bas de page

Même si elles n'existent plus depuis longtemps, il subsiste dans l'imaginaire collectif que tous les contrats d'assurance comportent des lignes de bas de page, écrites en petits caractères et listant des clauses permettant de ne pas payer ce que l'assuré pensait percevoir. Étonnamment, les politiques Sécurité pourraient parfois en remontrer à ces contrats d'une autre époque. Pas de petites lignes certes, mais des exceptions à la règle pas toujours si connues : "tous les PC sont sécurisés sauf dans telle entité", "tous les utilisateurs ont une authentification forte sauf les VIP", etc. Ces exceptions, souvent fruits d'impossibilités techniques dues à un historique ou de complexités politiques difficiles à faire disparaître, fragilisent à la fois le système d'information et la position du RSSI.

Pour l'assureur, ce sont justement dans ces zones grises que se trouvent fort probablement les causes des incidents futurs, et il voudra donc logiquement obtenir un inventaire exhaustif avant de proposer un contrat. Là encore, ce regard externe doit pousser

l'entreprise à se poser les bonnes questions sur le périmètre à assurer : est-il raisonnable d'assurer un périmètre au niveau de sécurité incertain, en sachant que l'on ne saura pas démontrer à l'assureur la mise en œuvre des bonnes pratiques ? A l'inverse, l'identification de ces zones "non assurables" peut permettre une prise de conscience et déclencher un vrai plan d'actions dont la réalisation est nécessaire pour les assurer.

Conclusion

Il apparaît donc évident que l'assureur, en posant les questions visant à estimer son propre risque financier à la signature d'un contrat, contribue à une meilleure appréciation par l'entreprise de ses cyber-risques, en imposant une quantification pécuniaire systématique de l'impact d'un incident. Cette meilleure appréciation, couplée à une mesure précise de l'efficacité supposée des actions de réduction des risques, favorisera l'établissement de plan d'actions plus pertinents.

Ces éléments nous semblent les bases indispensables pour engager des négociations contractuelles permettant à chacun de remplir au mieux son rôle : d'un côté, l'entreprise qui se doit d'assurer la résilience en cas d'incident de cybersécurité et de l'autre, l'assureur accompagnant son client dans la couverture de ce nouveau type de sinistre.

La cybersécurité s'est aujourd'hui débarrassée de sa réputation de sujet purement informatique - et c'est heureux - mais les RSSI continuent encore trop souvent de raisonner en informaticiens. Nous devons résolument nous ouvrir aux autres expertises, en commençant par celle des assureurs, la résilience de nos entreprises n'en sera que meilleure.