Une matrice pour anticiper et traiter les risques cyber

Gérard PELIKS
Chargé de cours cybersécurité dans les écoles d'ingénieurs et instituts
Membre de l'ARCSI

Dans le cyberespace, l'Information est en grand danger

Le cyberespace est le lieu de tous les dangers. Chaque jour apporte son lot d'attaques qui minent la confiance qu'on peut accorder aux fournisseurs, aux partenaires, et qui est accordée par les clients, et les employés. Le nombre d'attaques explose. Organisations grandes et petites, particuliers, tous sont menacés. Parfois la survie de l'organisation est mise en péril quand elle n'a plus accès à son Information qu'on trouve chiffrée par un cryptovirus en vue de demander une rançon, ou volée par un concurrent qui prend un avantage concurrentiel. Le risque est bien réel, il est omniprésent. Il est indispensable pour une organisation de maîtriser le risque numérique qui pèse sur son Information, pour générer la confiance, et plus pragmatiquement pour continuer à exister. De plus, bien maîtriser le risque peut également générer un avantage compétitif.

Mais comment appréhender le risque qui pèse sur son Information et sur les systèmes qui la gèrent ? S'il est admis que le « risque zéro » ne sera jamais atteint, il est aussi évident qu'on ne peut tout protéger. Par quoi commencer pour gérer cette situation ?

Cartographier les risques

Commencer par cartographier ses ressources numériques pour déterminer où se trouvent les gisements d'informations les plus sensibles est une bonne pratique. C'est là où se trouvent les informations de valeur qu'il faut placer les contre-mesures dont on dispose pour les protéger, et là seulement car on ne peut tout protéger. Savoir où se trouve son information est d'autant plus indispensable que de plus en plus souvent l'Information ne se trouve plus dans l'entreprise mais est confiée à un Cloud public, privé ou hybride. Il est indispensable d'élaborer dès le départ un cadre de gouvernance du risque numérique, pour ne pas se trouver fort dépourvu quand un problème est venu.

Savoir comment réagir à une cyberattaque devient bien plus facile quand on a prévu à l'avance la conduite à tenir pour en diminuer les effets ou pour la rendre moins probable. Plus que le produit « gravité des conséquences, vraisemblance que le risque arrive », pour connaître la criticité du risque, il est d'avantage intuitif de constituer une matrice des risques et un fichier des actions associées. Cette matrice de hiérarchisation des risques cyber est très utile si elle est constituée avant qu'il ne soit trop tard. Prenons conscience que, comme le dit un dicton, « les tuiles qui protègent de la pluie doivent toutes avoir été posées par beau temps ».

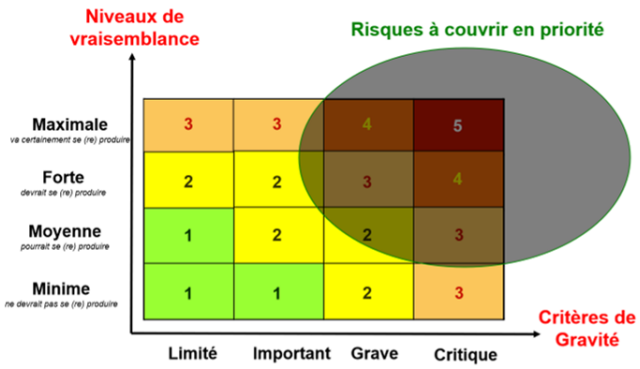
Pour constituer la matrice, dite diagramme de Farmer, traçons sur un axe horizontal, la criticité du risque, suivant, par exemple, quatre critères : risque limité,

risque important, risque grave et risque critique. Un risque est limité s'il n'entraine pas de conséquences insupportables quand l'attaque se produit. Un risque est important s'il gène le travail mais sans l'arrêter, ou si les clients s'en aperçoivent mais peuvent à la limite l'admettre. Un risque est grave si le travail est fortement perturbé et si les clients et la presse commencent à se poser des questions sur le sérieux et la compétence de l'organisation qui subit l'attaque. Un risque est critique s'il peut causer la disparition de l'organisation.

Il est bien évident que si un risque est critique mais ce qui peut le causer n'arrive (n'arrivera ?) jamais, on peut, peut-être, l'ignorer. Il est aussi évident que si un risque est limité, mais les attaques qu'il prévoit deviennent assez gênantes quand elles se produisent trop souvent, il vaut mieux en tenir compte dans la mesure du possible, si d'autres priorités n'impliquent pas de reporter l'action à plus tard. Mais la priorité reste de traiter en priorité les risques qui entrainent les conséquences les plus graves. En un mot il faut tenir compte d'un seuil d'acceptation des risques et avoir pensé à l'avance ce qui peut être fait pour en diminuer les effets.

Alors traçons sur un axe vertical le niveau de vraisemblance qu'un risque se concrétisera par une attaque. Prenons encore, par exemple quatre critères : Vraisemblance minime, vraisemblance moyenne, vraisemblance forte et vraisemblance maximale. Une vraisemblance minime indique qu'une attaque a très peu de malchance d'arriver. Une vraisemblance moyenne indique que la concrétisation de la menace par une attaque pourrait bien se produire. Une vraisemblance forte indique que l'attaque devrait se produire. Enfin une vraisemblance maximale implique que non seulement l'attaque va certainement se produire mais aussi se reproduire.

En fonction de ces quatre critères de gravité et de ces quatre critères de vraisemblance, on peut bâtir un tableau dit « matrice de criticité » où, dans chaque cellule, on inscrit une quantification des risques, de 1 à 5.



Dans les cases 1, le risque est mineur, et n'impacte ni les clients, ni le travail, ni l'information, on peut donc placer les contre-mesures ailleurs, on admet le risque sans le traiter. Dans les cases 2, le risque est faible, les perturbations subites resteront acceptables, on peut ne pas le traiter, au moins dans l'immédiat. Cases 3, le risque est moyen, il a une incidence gênante, il faut le traiter. Cases 4, le risque est fort, il faut traiter la concrétisation de ce risque le plus rapidement possible. Dans la Case 5, en haut à droite, le risque est critique, l'incidence est majeure, il faut pouvoir le traiter immédiatement sinon il y a possibilité de disparition de l'organisation.

Dans un autre document, on décide de la conduite à tenir pour chaque case et qui il faut impliquer pour le traiter. La conduite va de (cases 1) « on accepte, on ne passe pas de temps dessus » à (cases 5) « on traite le problème immédiatement, toutes affaires cessantes » C'est à partir des cases 3 qu'il faut placer des contre-mesures et prendre les décisions qui s'imposent quand l'attaque se produit. Il est bon également de quantifier les effets des risques, par exemple décider dans quelle case on met tel problème quand il entraine telle perte financière, tels jours de retard ou tel nombre de clients lésés, blessés ou simplement perdus.

Il faut également tenir compte, pour chacune des cinq quantifications, de la dimension « métier ». On ne traite pas le risque de la même manière chez un constructeur aéronautique que dans une banque, une société d'assurance, de transports, un établissement de santé ou un média. Une matrice des risques ne peut se justifier qu'au niveau d'une entreprise ou d'un service, mais n'est en aucun cas une matrice théorique unique qui sert de modèle dans tous les cas.

Il faut aussi décider à l'avance si les conséquences de chaque risque sont à traiter au plus haut niveau de l'organisation ou seulement au niveau des experts techniques ou juridiques, ou ne sont pas à traiter du tout. De plus, les menaces évoluent, donc les risques aussi. Ces travaux doivent être mis à jour au moins sur une base annuelle.

Deux exemples

Prenons comme premier exemple les risques qui pèsent sur l'information d'un journal ou d'une chaîne de télévision, et analysons les dangers qu'une cyberattaque fait peser sur son image. Sur le fichier associé à la matrice des risques, le risque des cases « 1 » n'implique pas de médiatisation, le média peut l'accepter. Le risque des cases « 2 » entraine un risque modéré (faible tirage d'une presse locale, très peu d'impacts dans les réseaux sociaux…) on peut aussi l'accepter. Le risque des cases 3 implique une médiatisation limitée mais les risques des cases 4, et surtout ceux de la case 5, causent une dégradation durable de l'image du média, la presse internationale reprend l'information corrompue ou dévoilée et l'atteinte à la réputation du média peut entrainer sa disparition, faute de lecteurs, en plus des sanctions.
Comme autre exemple, prenons les menaces sur l'Information d'une société de transport. Dans les cases 1, il n'y a pas d'impact visible sur la disponibilité ou l'intégrité du système d'Information, l'attaque n'est pas visible et n'entraîne rien de sérieux, on l'ignore, ou en tout cas on peut-on tenir compte plus tard. Dans les cases 2, l'activité est un peu désorganisée et des clients sont assez mécontents, le risque est à considérer, mais on peut le traiter dans un deuxième temps. Dans les cases 3 et dans certaines cases 4, la désorganisation est importante et les usagers sont forts mécontents. Il faut agir. Dans certaines cases 4, et en tout cas dans la case 5, le service est arrêté, il y a peut-être eu un terrible accident avec des victimes. Il faut le traiter immédiatement et il est nécessaire de déclencher une cellule de crise.

Plus c'est modulaire, plus c'est efficace

On peut aussi établir de telles matrices sur les atteintes à chacune des facettes de son Information : sa disponibilité, son intégrité, sa confidentialité et sa traçabilité, et ce pour tous les process qui manipulent cette information. Plus la quantification du risque est modulaire, plus elle peut être efficace.
Avec cette matrice, et le fichier des conduites à tenir, complexes à établir certes pour une grosse organisation mais fort utiles, on sait à quoi s'en tenir, on connait les actions à mener, à quel niveau, immédiatement ou en différé, et s'il est indispensable de réunir une cellule de crise, mettre en œuvre son plan de continuité ou de reprise d'activité. Il faut disposer de ces plans, et activer sa police d'assurance si le risque numérique, direct et indirect, est en parti couvert. Et tout cela augmentera la résilience, donc la compétitivité de son organisation.
Mettre au point cette matrice et le fichier associé dans lequel sont détaillées les actions qui s'imposent est un travail d'experts, qui doit réunir techniciens, juristes, service du personnel et être validé par la direction.

La cybersécurité doit devenir la norme, et la classification des risques est le premier outil pour diminuer la gravité des impacts d'une attaque, et diminuer également la probabilité que cette attaque se produise. Et la sensibilisation de tous aux dangers du cyberespace est la deuxième priorité.