



Article de Philippe Giroux
Directeur de la pratique de sécurité
ESI Technologies

L'analyse de risque, un élément fondamental de la sécurité informatique

Trop souvent négligée, particulièrement par la PME, l'analyse de risque n'en constitue pas moins un outil essentiel dans la chaîne de la sécurité informatique. Elle est même l'une des premières étapes et forme le principal moyen pour optimiser la sécurité. Si optimiser signifie faire le maximum, cela signifie aussi le faire avec le minimum de ressources possibles. Tous ayant intérêt à avoir une sécurité appropriée, et tous ayant intérêt à réduire au minimum leurs coûts, l'analyse de risque est donc de première importance pour tous les environnements.

La gestion du risque a depuis fort longtemps été intégrée aux entreprises de tous genres. Maintenant que les ordinateurs sont entrés dans les entreprises, le risque informatique doit être pris en considération. De plus, l'informatique étant maintenant en charge de plusieurs opérations critiques, si ce n'est toutes, le risque informatique devient l'un des principaux risques de l'entreprise d'aujourd'hui.

L'analyse consiste à évaluer le risque que fait peser une menace en fonction de deux facteurs, la probabilité et l'impact. Lorsque l'impact est évalué en dollars, on parle d'analyse quantitative, autrement on parle d'analyse qualitative. Les deux facteurs du risque se multiplient pour donner le niveau de risque. À probabilité élevée de causer un lourd dommage, le risque est maximum, l'idéal étant une faible probabilité qui, malgré tout, ne causerait pas de dommage significatif.

Les menaces sont de plusieurs types. Des exemples sont la malveillance, l'erreur et l'accident. Dans le cas de la malveillance, la concrétisation de la menace est voulue et les efforts requis sont fournis. La menace est à la fois ciblée et non-aléatoire. Pour sa part, l'erreur est aléatoire, mais demeure ciblée. En effet, pour qu'une erreur soit commise, il faut d'abord qu'il y ait eu action. Ainsi, l'erreur ciblera surtout les données en cours de manipulation. Finalement, l'accident est à la fois aléatoire et non-ciblé, pouvant se produire dans toutes les conditions. Le bris d'un disque dur est un exemple.

Si les menaces peuvent être de plusieurs types, les ressources impactées par ces menaces sont tout aussi variées : serveurs, bases de données, édifice, système de câblage et plus encore. Avec autant de facteurs, menaces, ressources et plus, il devient évident que le champ de l'étude peut être très large. C'est pourquoi, dès le début du processus, il est essentiel de définir un périmètre et de s'y limiter. On déterminera ainsi les types de ressources qui seront prises en compte ainsi que les types de menace qui seront évaluées.

Le choix des personnes qui formeront l'équipe de projet est également une étape très importante. En effet, l'analyse de risque ne doit pas être le fruit d'un travail solitaire. Au contraire, il s'agit d'un travail d'équipe qui nécessite la participation de plusieurs acteurs-clefs : représentants des utilisateurs, de l'informatique, de la haute direction, de la sécurité informatique, des relations avec le public et potentiellement plus encore. Bien entendu, le travail gagne à être piloté par un expert de l'analyse de risque afin de guider les participants vers les bonnes questions et réflexions pour obtenir un plan d'action optimal.

Enfin, le choix d'une méthodologie d'analyse est aussi à faire. Il existe quelques méthodes pouvant guider les entreprises dans cette tâche; Méhari et Octave en sont deux exemples. Les organisations feront leur choix en se fondant sur des critères comme les fonctionnalités offertes, les preuves d'efficacité, l'évolutivité, la souplesse et l'universalité.

Au Québec, la norme Méhari (MEthode Harmonisée d'Analyse de RIques) est assez répandue, notamment dans le secteur public. Développée en France par le Clusif (Club de la Sécurité des Systèmes d'Information Français), elle a acquis une maturité appréciable. Son principal avantage, outre les bases de connaissance, réside dans son formalisme et dans les métriques proposées.

Conçue par le Software Engineering Institute de l'Université Carnegie-Mellon, la méthode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) connaît elle aussi une certaine popularité auprès des organisations québécoises. Sa simplicité de mise en œuvre en fait un outil efficace.

Enfin il est toujours possible de développer sa propre méthodologie en s'inspirant de ce qui existe. Plusieurs publications traitent du risque informatique et proposent des solutions pour l'appréhender. Le NIST (National Institute of Standards and Technology) a écrit l'un des documents de référence dans le domaine, 'Risk Management Guide for Information Technology Systems'. On peut également citer le livre 'Le Risque Informatique' de Jean-Philippe Jouas, un des concepteurs de la méthode Méhari.

Le travail de l'équipe d'analyse de risque consistera à définir les conséquences pouvant affecter les ressources du système d'information et à en mesurer l'impact. Une fois les pires conséquences identifiées, les scénarios qui produiraient ces conséquences sont envisagés. L'équipe pourra ensuite concevoir des mesures de mitigation qui permettront de réduire le risque en fonction des deux facteurs le composant. Certaines mesures chercheront à réduire la probabilité alors que d'autres tenteront de réduire le dommage. La priorité des risques à atténuer pourra être établie en fonction des besoins de sécurité de l'entreprise, besoins normalement exposés dans sa politique de sécurité.

En exemple d'une telle démarche, voici ce qui pourrait être fait à l'ouverture d'un projet de portail Web dédié au commerce électronique. L'expression de besoin insisterait sur la disponibilité et l'intégrité avant tout. Les paiements étant délégués à chaque fois vers un autre système, les besoins de confidentialité, d'authenticité et d'imputabilité pourraient être limités.

Quelques scénarios qui porteraient atteinte à la disponibilité pourraient être une attaque de déni de service par inondation, une mise à jour du site Web qui tournerait mal, ou encore une coupure d'alimentation électrique. Pour contrer la malveillance, une entente pourrait être prise avec le fournisseur d'accès Internet pour garantir une réaction adéquate en cas d'attaque de la sorte. Cette mesure vise directement la réduction du dommage. L'erreur pourrait être modérée par une procédure de sauvegarde rigoureuse, encore plus stricte au moment des mises à jour. Là aussi, la mesure cherche à réduire les dommages. Finalement, une alimentation électrique d'urgence pourrait être ajoutée à tous les composants critiques de la communication, réduisant la probabilité de perdre toutes les alimentations à un seul moment.

Il existe plusieurs solutions pour résoudre les problèmes d'un risque trop élevé. Comme indiqué dans les exemples plus haut, des mesures préventives appropriées peuvent être prises pour réduire la probabilité et / ou le dommage associé à la menace en question. Il est aussi possible de transférer ce risque à une autre personne par le biais d'une assurance. Finalement, il est aussi possible de revoir les processus d'affaires pour les ajuster à un niveau de risque accepté mais plus élevé que prévu.

Une fois les risques et menaces identifiés et gérés, il est important de documenter tout le processus et les risques résiduels. Les risques résiduels sont formés autant des risques qui n'ont pas été atténués que des niveaux auxquels les autres risques ont été diminués. Cette documentation permet autant de ne pas oublier les risques résiduels que d'accélérer tout le processus lors d'une prochaine analyse de risque quand un nouveau projet majeur démarrera.

Une raison qui motive souvent l'entreprise à faire une analyse de risque est que, après une période d'investissements parfois hasardeux pour mettre en oeuvre une sécurité périphérique, elle a besoin d'avoir une vision globale de son risque informatique réel. L'analyse de risque propose alors une approche plus réfléchie et mature tout en offrant le recul nécessaire à l'élaboration d'un plan stratégique pour la sécurité des systèmes d'information.

Le meilleur moment pour mener une analyse de risque est lors du lancement de nouveaux projets informatiques. Qu'il s'agisse de la conception d'un nouvel applicatif, de l'acquisition d'un nouveau logiciel ou de la centralisation de plusieurs systèmes sur une seule plate-forme, il sera toujours bénéfique pour l'entreprise de procéder à cette réflexion en prenant le recul nécessaire.

L'analyse de risque peut aussi être réalisée dans un cadre plus large lorsqu'il s'agit d'élaborer un plan stratégique ou un schéma directeur de la sécurité des systèmes d'information. Dans ce cas, on analysera l'ensemble des processus d'affaires vitaux de l'entreprise de manière à avoir une idée précise de ses besoins, dépendances, sources de revenus et autres éléments majeurs.

Contrairement à ce que plusieurs pourraient penser, réaliser l'analyse de risque d'un projet et aboutir à un plan d'action demande relativement peu de temps. Il y a évidemment des variations selon l'étendue et le champ de l'application mais très souvent, il suffit de quelques jours pour effectuer ce travail. Les coûts ne sont donc pas exorbitants.

L'analyse de risque est une étape de la sécurité dont l'importance n'a d'égal que son actuelle absence lors de très nombreux projets. Outil d'optimisation par excellence pour la sécurité, l'analyse de risque faite en début de projet permet autant d'offrir une réelle sécurité que d'éviter le gaspillage de ressources humaines et financières.

Avant de faire de la sécurité, il faut savoir qu'est-ce que la sécurité. Or, il n'y a pas deux environnements pour lesquels la sécurité a la même signification. La disponibilité sur ceci, la confidentialité sur cela, parer la malveillance ici, être tolérant aux pannes accidentelles là, la sécurité est trop large pour penser la déployer à son maximum en tous ses points. L'analyse de risque est ce qui permettra de donner sa bonne définition à la sécurité. Ce ne sera qu'une fois l'objectif défini qu'il pourra être atteint.