Un nouveau regard en matière d'analyse de risques

«Si, dans le passé, certains dirigeants d'entreprises avaient peur d'analyser formellement leurs risques, car tout manquement à un traitement adéquat de ces risques pouvait plus facilement leur être reproché, une telle approche n'est plus compatible ni avec les principes de management moderne, ni avec les exigences légales», atteste Carlo Harpes, directeur de la société itrust consulting, qui vient de mettre sur le marché une application Web novatrice à même de comparer les pertes financières attendues, par exemple d'un vol de données avec les coûts de la sécurité. Interview.

> "Malgré la loi sur la protection des données, peu d'entreprises au Luxembourg formalisent les risques qu'elles ont à gérer"

M. Harpes, itrust consulting a pour vocation d'aider ses clients à protéger leurs informations contre la divulgation, la manipulation ou l'indisponibilité. À ce titre, votre société propose entre autres des services d'analyse de risques. Quelles sont les principales problématiques que vous rencontrez chez vos clients à ce niveau?

En guise de rappel, la « gestion des risques » consiste tout d'abord à apprécier, c'est-à-dire, à identifier puis analyser et enfin évaluer tout ce qui peut mettre en danger les objectifs de l'entreprise. Ensuite, cette gestion doit traiter ces risques, c'est-à-dire les accepter, prendre des contre-mesures voire arrêter une activité. Enfin, la gestion inclue la communication sur les risques afin que le personnel concerné, et même les clients, comprennent à tout moment les enjeux et prennent les bonnes décisions.

Lorsque je dois évaluer ce qui n'est encore jamais arrivé, comme une cyberattaque visant mon entreprise, je fais généralement des erreurs, ou, plus précisément, je dois maintenir une marge d'incertitude. Certaines entreprises ont peur de documenter une évaluation des risques, car cette dernière contient nécessairement des erreurs. D'autres le font seulement pour répondre aux exigences légales, mais oublient de maintenir la rigueur de l'évaluation dans le traitement et la compréhension des risques par les dirigeants.

Qu'est-ce qui explique que l'analyse de risque est aujourd'hui à l'ordre du jour du management?

Bizarrement, ce ne sont pas les dispositions légales : la loi de 2002 sur la protection des données à l'article 22 exige que « Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données ». Il en découle que sans pièce justificative sur les risques encourus, c'est-à-dire sans analyse formalisée, il ne peut pas justifier que les mesures prises sont adéquates, et donc qu'il a rempli ses obligations légales. Après un vol de données, il a l'évidence que le niveau de sécurité était insuffisant ; il ne peut plus justifier a posteriori le bien-fondé de son niveau de sécurité. Vous voyez qu'il est simple par toute personne lésée d'un vol de données de prouver une non-conformité légale au responsable du traitement si ce dernier ne peut se justifier par une analyse de risque en bonne et due forme validée avant le sinistre. Pourtant, les organisations responsables de traitement ayant mis en plan une telle approche sont plutôt rares.

Carlo Harpes

Mais ce qui vient de changer, c'est que les régulateurs luxembourgeois, comme la CSSF et la CNPD, demandent à voir les rapports d'analyse et de traitement. C'est ce travail préventif qui porte ses fruits, plutôt que le travail répressif et l'indication de sanctions exagérées.

N'oublions pas non plus l'amélioration des pratiques de management citée ci-avant. La gestion du risque permet de mieux évaluer l'utilité de la sécurité, en justifier les coûts, et planifier les dépenses futures, en fonction du niveau de risque accepté. Et cette démarche assure d'être mieux préparé aux attaques.

Face à ce constat, que préconisez-vous?

Si l'on se réfère aux recommandations de l'ENISA, l'agence européenne de la sécurité des réseaux et de l'information, un bon projet d'analyse de risques s'établit en concertation entre les collaborateurs en interne, qui connaissent bien la problématique, et des experts externes, qui connaissent la méthodologie et qui peuvent s'assurer de la cohérence des évaluations par rapport à d'autres organisations similaires.

Pour venir en aide et faciliter ces analyses, itrust consulting mise depuis des années sur le développement d'un outil, baptisé 'TRICK Service', dont l'application Web vient d'être finalisée et mise sur le marché.

Comment est née l'initiative?

Grâce à notre implication dans de multiples projets de recherche financés soit par le ministère de l'Economie, soit par la Commission européenne tels que BUGYO Beyond, CockpitCI ou TRESPASS, nous avons été à même de développer de plus en plus de fonctionnalités utiles pour la mise au point d'un outil d'abord développé en Excel, puis en application Web. Ces fonctions sont le calcul de rentabilité, le ficher de structuration des discussions sur les menaces et les risques, les coûts des processus de sécurité selon ISO 27001 et des mesures d'ISO 27002, les exigences luxembourgeoises pour la dématérialisation et l'archivage, le cloud, les seuils et registres préconisés par la CSSF, l'évaluation de la maturité, etc.

Quelle est la vocation de cet outil et quelles sont ses particularités?

La vocation première de 'TRICK Service' est de guider une organisation dans la mise en place de son système de gestion de la sécurité. À cet effet, l'application estime d'un point de vue quantitatif les probabilités et les impacts de certains scénarios de risques appliqués aux assets de l'entreprise.

Par ailleurs, TRICK Service a également pour mission de documenter le niveau de sécurité déjà implémenté par rapport à plusieurs référentiels de sécurité ISO 27002, PSDC, 27799, etc., avant de chiffrer le coût d'implémentation de chaque mesure qui fait défaut.

Pour finir, un modèle mathématique permet de lier la sécurité au scénario de risque, par l'utilisation des facteurs de réduction de risques, ceci afin d'estimer la rentabilité de chaque mesure de sécurité.

Ces éléments permettent de dériver un plan de traitement qui s'avère plus utile que la pure connaissance des risques. Précisons que nous avons conçu cet outil de sorte à ce qu'il puisse se conformer aux exigences tant du régulateur luxembourgeois que des normes ISO 27001.

Qu'est-ce qui distingue votre produit de ceux de vos concurrents?

Il existe sur le marché un certain nombre d'applications très connues telles qu'EBIOS, MEHARI, verinice ou encore MAGERIT. Force est de constater que malgré l'engouement suscité par ces outils sur leurs marchés nationaux respectifs, ceux-ci affichent une charge de travail impressionnant dans l'utilisation, ce qui conduit les entreprises qui en ont fait l'acquisition à ne les utiliser qu'une seule fois. Ce faisant, ces entreprises ne maintiennent pas à jour leur analyse de risques, avec les dangers que cela suppose au niveau de leur sécurité.

Avec notre outil web TRICK Service, nous avons pris le contre-pied de cette méthode. Nous proposons un outil nettement plus pragmatique et précis qui ne se borne pas à définir un simple niveau de risque ou d'établir un système de points de risques tel que le proposent nos concurrents, mais une indication des coûts de mise au point et des coûts récurrents, pour chaque phase d'implémentation, et l'indication du risque résiduel exprimé en perte moyenne en k EUR à attendre sur une année.

Parfois, des clients le considèrent aussi comme concurrent à l'outil MONARC de SMILE GIE. Or il s'avère que MONARC, que nous utilisons également, couvre d'autres besoins, et déploie son potentiel en l'appliquant à de multiples organisations similaires, comme les administrations communales, alors qu'il ne permet pas de chiffrer des coûts et des rentabilités.

itrust consulting
55, rue Gabriel Lippmann
L-6947 Niederanven
Tél. : 26 176 212
Contact : info@itrust.lu
www.itrust.lu