La Sécurité du Système d'Information (« SSI »), un métier ?

Patrick Kineider,
Animateur du Groupe de travail « risques et sécurité des SI »

Dans le domaine informatique des entreprises et des administrations, en matière de sécurité du système d'information, comme en termes de technologie, l'évolution a été constante depuis le milieu du XXe siècle : informatique lourde et grosses applications, avec ses plans de secours et de continuité ; micro-informatique avec les premiers virus ; réseaux locaux puis globaux, avec des attaques malveillantes. La montée en puissance de l'Intranet et de l'Internet, puis le début de la « convergence informatique/télécom », ont incité les entités à investir et à s'organiser en termes de SSI, dans un monde ouvert, interactif, extrêmement concurrentiel.
La personne incontournable en termes de SSI est le Responsable Sécurité du Système d'Information et de Télécommunications – jadis il s'agissait du RSSI (c'est-à-dire le RSSIT, sans les télécommunications). Il est chargé de proposer et de gérer la protection technique et organisationnelle des informations et « processus » sensibles, vulnérables, et d'éviter, en organisant des sensibilisations appropriées, les gestes utilisateurs non conformes à l'éthique (personnelle ou professionnelle).
Les tâches liées à la Sécurité des Systèmes d'Information (SSI) constituent-elles des métiers en soi nécessitant des connaissances poussées, ou de simples fonctions d'appui ? C'est à cette question que les lignes qui suivent s'efforcent de répondre.

Rôle et position du RSSIT

On l'a vu, le RSSIT a pour rôle d'assurer la sécurité du « patrimoine informationnel » (données informatiques, écrites, ou téléphoniques) contre les risques.

Par conséquent, il doit connaître la « valeur » et surtout savoir évaluer la disponibilité, l'intégrité, la confidentialité et la traçabilité (les « critères DICT[1] ») des données auxquelles ont accès les utilisateurs sur leur poste de travail. Il est le garant de la connaissance par tous et de l'application quotidienne des règles communément appelées « chartes d'utilisation », ainsi que des contrats de confidentialité (salariés de l'entreprise ou intervenants extérieurs). Il effectue, ou commande, des audits méthodologiques.
Il a un rôle d'appui et de conseil auprès du management, mais aussi auprès des métiers, ainsi que des exploitants informatique et télécom. Il coordonne la mise en place d'outils de sécurité passive (mots de passe, cryptage, digicodes,..). Il analyse les incidents informatiques notoires, les situations de crise, etc.
À noter que la sécurité de l'information papier est gérée de manière très spécifique suivant les entreprises car il n'y a pas de modèle de référentiel de sensibilité des divers types de documents, ou d'organisation des archives par exemple. De la même façon, tant que les télécommunications n'étaient pas numérisées (système de « voix sur IP »), la protection des donnés « voix » était souvent très élémentaire.

Une mission SSI peut-elle être assortie d'indicateurs ? Il en existe quelques-uns : le nombre d'attaques malveillantes, ou le taux de logiciel antivirus ou de logiciels de chiffrement, installés sur les postes et serveurs. À noter que les managements préfèrent souvent les « paramètres de gestion » aux paramètres de « sinistralité » proprement dits.

Exemples

Dans une grande banque, si la salle des machines est détruite par un incendie, l'exploitation déclenchera un « Plan de Continuité d'Activité » en repliant ses équipes sur un site de secours. Ce dernier est constitué de postes de travail sur lesquels les utilisateurs pourront poursuivre leur activité, à l'aide de copies sécurisées des logiciels et des données concernées. Tant qu'un site « propre « n'est pas entièrement reconstitué, l'ensemble tournera ainsi sur le site de secours.

Dans une entreprise de commerce en ligne (telle que : La Redoute, la FNAC, etc..), le rôle du RSSIT sera, entre autres, de garantir la fiabilité et la confidentialité des transactions côté fournisseur, entre autres, en maintenant le système informatique de « gestion des commandes » et en finalisant le système de contrôle d'existence de la carte de crédit de l'acheteur.

[1] *DICT comme Disponibilité, Intégrité, Confidentialité, Traçabilité*

La fonction, les moyens

D'après ce qui précède, le poste de RSSIT devrait être, de préférence, occupé par un salarié de l'entreprise ayant une expérience de celle-ci et de ses « enjeux », mais pas nécessairement des compétences informatiques ou télécom. Bien souvent la SSI sollicitera l'aide de « professionnels » (exploitants informatiques salariés ou sous-traitants, sociétés de service spécialisées,..).Dans la plupart des entreprises, le RSSIT est rattaché, soit à la Direction des Systèmes d'Information, soit à la Direction générale. Il participe ainsi aux divers plans d'action de l'entreprise (managérial, financier,..). Ce poste est, d'ailleurs, souvent confié à un Directeur. La SSI est un centre de coût d'importance variable, qui peut être indépendant ou non.

Classiquement, la sécurité des personnes et des locaux, tout comme la sécurité informatique, sont considérées comme des freins, soit à l'activité, soit à la performance ; le rôle du RSSI est de porter, par des arguments simples et compréhensibles de tous, la nécessité de sa prise en compte, il doit donc avoir des qualités personnelles de contact.

En conclusion

Au vu de ce qui précède, le RSSI apparaît dans l'entreprise comme une fonction d'appui c'est-à-dire transverse, éventuellement rattachée à un processus du même type. Elle n'en reste pas moins stratégique dans un milieu globalisé, ouvert, interactif.

patrick.kineider@numericable.fr