

Les enjeux de la sécurisation des données

Sécurité

Posté par : JulieM

Publié le : 19/10/2016 14:30:00

Nous y revenons régulièrement : la somme des données collectées au niveau du SRM (Supplier Relationship Management) est très importante et le partage croissant d'information entre les entreprises et leurs fournisseurs au travers de solutions collaboratives laisse présager d'une tendance à la hausse. Importantes par le nombre, ces données le sont aussi par leur caractéristique stratégique et sensible, un sujet anxieux qui concerne toutes les sociétés, quel que soit leur domaine d'activité.

À

Enjeux liés à la sécurisation des données

D'abord, l'enjeu majeur est lié à la fuite des données mais aussi à leur corruption. Bien souvent, l'origine de ces incidents est le résultat d'une intervention humaine plus que celle de problèmes techniques ; le niveau de complexité des processus internes et le nombre d'intervenants augmentant naturellement ce risque.

Les données achats, incluant données contractuelles et données techniques, sont critiques pour une large part, ce qui implique une nécessaire prise de conscience en la matière.

L'enjeu moins direct est celui du frein au changement : par méconnaissance des solutions SRM et de leur fonctionnement, beaucoup de directions générales ou de directions achats hésitent à mettre en place un outil qui représente pour eux un risque, dans la mesure où il ouvre les canaux à l'interne, mais aussi à l'externe, la plateforme d'échange étant ouverte aux fournisseurs.

Cette ouverture sur l'extérieur peut entraîner une méfiance des sociétés qui ne veulent pas voir leurs données exposées au risque de perte, de piratage ou de détérioration. Il est donc important de s'appuyer sur des environnements permettant de pallier ces risques.

Le risque de sécurité, successeur naturel de l'opportunité innovation

Enfin, la sécurisation des données est une question qui intervient de façon tout à fait récente dans beaucoup d'entreprises, y compris au niveau des DSI. Il s'agit du revers de la médaille de la transition numérique. On crée de nouveaux outils, et dans la foulée on prend conscience des risques qui y sont liés. À l'innovation, succède invariablement le risque, lui-même suivi par l'évolution des systèmes de protection.

On ne peut pas se prémunir d'un risque non existant, c'est pourquoi la sécurisation est une question qui appelle à la veille et à l'observation constante. L'arrivée des objets connectés (IoT) illustre bien cette question : on a commencé par connecter les objets, se pose seulement maintenant la question de la sécurisation de la data qui transite.

Comment prémunir les directions achats du risque lié à la sécurisation des données ?

Tout d'abord, il faut bien considérer qu'il est naturel que la protection des données ne soit une priorité que très récente. En effet, la technologie nous a amenés à savoir collecter, stocker, hiérarchiser et gérer des données, mais pas à prouver immédiatement les

limites de ces nouveaux systèmes.

On peut regarder du côté d'acteurs comme la NSA, qui utilise des criminels repentis pour tester et casser ses systèmes, pour appréhender la question de la sécurisation. Il faut pouvoir faire intervenir un œil extérieur pour chercher la faille de sécurité avec objectivité. Il est donc important de détecter cette faille et de trouver une solution au problème.

Autre clé : la sensibilisation des utilisateurs. Dans un premier temps, il est nécessaire de réaliser un audit des systèmes SRM et du processus achats dans l'entreprise sur des critères non standards, afin de comprendre les spécificités de la société. Il est alors possible de mettre en place une charte à l'attention des utilisateurs de la solution dans l'entreprise.

De la même façon, cela permet de transmettre la culture de la sécurité à travers le partage de bonnes pratiques en valorisant leur importance. Par exemple, changer de mot de passe tous les trois mois peut paraître contraignant, mais il faut faire en sorte de donner aux entreprises les moyens d'impliquer leurs collaborateurs en leur faisant prendre conscience des risques existants. Confirme Franck Le Tendre, Directeur Général France de SynerTrade