

Fuite de données, les conseils de NES (...)

La fuite ou le vol d'information, thème plus que jamais d'actualité, est un phénomène qui n'est pas du tout récent. En effet, profitant de l'essor des nouvelles technologies, le SI a évolué en laissant souvent de côté ces aspects.

Les protagonistes - toutes personnes ayant accès aux données du SI de l'entreprise et/ou disposant de moyens de les détourner durant leur transport - utilisent les vecteurs classiques que sont les clés USB, le mail, pour exfiltrer ces données.

Certes toutes les entreprises n'ont pas le même enjeu. Mais quel manager ou patron d'entreprise resterait indifférent s'il voyait son fichier client, ses rapports financiers, ses contrats.... aller chez le concurrent ou tout au moins les voir divulguer sur la toile ?

La difficulté pour les entreprises est l'identification, la classification puis l'organisation des données dites sensibles. Les moyens d'y parvenir sont multiples :

1/ définir au sein de l'entreprise les données dites sensibles ou confidentielles.

Tous les salariés n'en n'ont pas la même notion. Du manager à la secrétaire susceptible d'y avoir accès, il peut y avoir un « gap » important.

2/ se doter de process clairs et homogènes concernant le traitement et stockage de ces données : l'Encryption des fichiers et/ou des répertoires cibles seront de mise dans ce cas par exemple.

3/ Opter pour une traçabilité maximale selon le tryptique " qui fait quoi, quand, comment" sur au moins les supports de stockage hébergeant des données sensibles.

4/ interdire les vecteurs de transport type clé usb personnel, postage de données sur les sites sociaux, Webmail,....

Par ailleurs, les solutions actuelles dites de DLP, si elles semblent abouties fonctionnellement présentent parfois des anomalies ou incompatibilités sur le plan opérationnel. Elles présentent encore beaucoup de faux positifs notamment, leur complexité de déploiement et d'administration n'est pas en reste.

NES préconise une approche « anti bricolage » dans ce domaine. L'enjeu est tel parfois que la remise en cause de l'organisation du SI et de certains de ses composants doit pouvoir être envisagée si l'on veut aboutir à un socle propice et efficace contre la fuite d'information.

Par exemple, on peut dans un 1er temps imaginer le stockage des fichiers plats de l'entreprise (relatifs aux informations sensibles) dans des « container » sécurisés spécifiques et dédiés à cet effet. Les mécanismes de contrôle d'accès classique doivent bien sûr être actifs (contrôle des accès USB, Webmail, proxy, ...). Pour les informations stockées dans des SGBD, nous sommes partisans de solutions logicielles simples, installées sur les serveurs de DB eux même pour contrôler/filtrer l'accès (SENTRIGO en est un parfait exemple).