Le coffre-fort électronique, premier pas vers le DLP

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 5 juin 2009

Spyworld Actu

Le DLP (Data Loss Prevention) encadre la protection des données sensibles de l'entreprise. On n'en est encore qu'aux premiers pas. Les rencontres du RIAM ont montré que les responsables sécurité débutent par des coffres-forts électroniques.

Les 5èmes rencontres du RIAM (Rencontres de l'Identity et de l'Access Management) ont eu lieu du 27 au 29 mai dernier. Organisées superbement par l'intégrateur Atheos, elles sont l'occasion privilégiée d'aborder des thématiques clés de la protection des systèmes d'information et les meilleures pratiques avec les responsables sécurité des plus grandes entreprises françaises.

On citera entre autres Carrefour, Areva, Michelin, Thomson, Société Générale, BNP Paribas, Crédit Agricole, Casino, Air Liquide, AGF, Louis Vuiton, Faurecia, EADS, etc ... Cette année plus de quatre vingt responsables étaient présents.

Les rencontres du RIAM (Rencontres de l'Identity and Access Management) réunissent les responsables sécurité des grandes entreprises (Ici, un des nombreux ateliers de travail)

Si les rencontres du RIAM étaient à l'origine conçues pour aborder les projets de gestion d'identités au sein des entreprises, un virage a été pris vers de nouvelles approches telles que le DLP (Data Loss Prevention) ou protection contre la fuite d'information. Plusieurs ateliers lui étaient consacrés, notamment animés par Utimaco (désormais racheté par Sophos) ou par Trend Micro.

Pour mémoire, le principe du DLP consiste à tracer les données selon leur importance stratégique (Il faut donc classer ses données) et leur cheminement dans le système d'information. Une solution de DLP doit savoir stopper des données que l'on transfère indument vers une clé USB (un agent logiciel sur le PC empêchera cette action) ou que l'on envoie par email (la passerelle de messagerie bloquera le message).

Afin de stopper des données, il faut mettre en place des règles de filtrage et d'identification de la criticité des données. Par exemple, si dans le modèle du document le mot "Confidentiel" apparaît, on pourra filtrer sur ce mot. Trend Micro propose également de filtrer sur "l'empreinte" (Fingerprint) du document, sur des expressions régulières (Regex), des mots clés (Keyword), un format, un template, ou des méta données.

Si certains RSSI ne sont guère convaincus par le DLP (« La question principale demeure la gestion des risques ! »), d'autres y voient une piste intéressante même s'ils ne l'ont pas encore déployé en interne. En fait, les solutions mises en place et décrites par de nombreux responsables sécurité lors des ateliers consistent à mettre en place des coffres forts électroniques. On a un peu l'impression de revenir quelques années en arrière, et cela sonne nettement moins moderne que le DLP mais cela paraît efficace. Ces coffres forts sont alors réservés à de petits groupes de personnes (dix à vingt personnes en général).

Les responsables sécurité tracent ensuite tous les accès à ces coffres forts électroniques. Toutes les modifications des documents sont effectuées au sein du coffre fort électronique. Par où débuter cette mise en oeuvre ? "Par le corporate parce que l'on ne pourra pas s'attaquer à tout et qu'ils sont sensibilisés" répond sans hésitation le RSSI d'une grande société. « Par exemple, le rapport annuel de l'entreprise ne doit pas circuler avant qu'il ne soit rendu public. Idem pour les documents définissant la gouvernance de l'entreprise. Il s'agit du plan stratégique pluri annuel, et de sa déclinaison en de multiples programmes » souligne-t-il. Il protège ainsi le coeur de la stratégie de son

groupe. Et il n'est pas le seul, plusieurs RSSI procèdent de la même façon pour les documents jugés les plus sensibles.

Pour aller au-delà, et mettre en oeuvre un DLP à l'échelle de l'entreprise, il faudra toutefois arriver à résoudre plusieurs questions. Comme le remarquait un RSSI qui a déployé un coffre-fort électronique : "L'informatique ne sait pas quelles informations sont confidentielles. Il n'y a que les métiers qui peuvent le définir. Or, ils sont peu motivés pour le faire". Dans sa propre entreprise, c'est le service juridique qui s'y est attelé. Il a défini la classification de ce qui est confidentiel ou pas. Cette classification doit être simple à comprendre et ne pas occuper un document de 50 pages. Et il s'agit d'un projet d'entreprise. "Nous avons une matrice de décision pour définir la classification de nos informations, cela permet de déterminer qui est le propriétaire de l'information, cela prend 2 pages" insiste un autre RSSI.

Les informations à accès restreint se voient chiffrées (sur les disques, les fichiers ou les bases de données), les autres ne l'étant pas. "Le chiffrement n'est pas du DLP", est alors intervenu un autre responsable sécurité, tout en admettant dans le même temps que le chiffrement était désormais mature, alors que le DLP n'en est encore qu'à ses débuts.

Ultime frein, note un autre responsable : "si l'utilisateur comprend qu'il ne peut plus envoyer un document par email quand il y met le mot confidentiel, très vite, il ne l'indiquera plus afin de travailler sans être bloqué". Une stratégie de contournement que l'on retrouve très fréquemment quand la sécurité devient un frein au business.

Post-scriptum :

http://securite.reseaux-telecoms.ne...