Recap 2005, stockage des données (II): le chiffrement s'est imposé

Récapitulons quelques-uns des faits les plus marquants qui ont impressionné les esprits en 2005: –

Time-Warner égare 40 cartouches qui comportent des données sur les employés – **Ameritrade Holding** perd plusieurs médias représentant les dossiers de 200.000 clients, – **Marriott Vacation Club** reconnaît avoir perdu les informations bancaires et de sécurité sociale de 206.000 partenaires, employés et clients, – **Bank of America** constate avoir perdu plusieurs cartouches représentant les informations confidentielles de 1,2 million de contacts, dont celles concernant un sénateur américain, – **Citigroup** admet la perte d'informations concernant 4 millions de personnes? Sans oublier les vols de PC portables, les actes de piratage ou d'intrusion qui, eux aussi, préoccupent de plus en plus. Et sans omettre le coût de «reconstruction» ou restauration de l'information, ou encore les amendes éventuelles et les dommages dus aux pertes financières associées. Pour ceux qui doutent encore, ils peuvent visiter un site américain spécialisé qui recense la plupart des sinistres reconnus, ayant provoqué la perte d'informations: www.privacyrights.org/ar/chrondatabreaches.htm. Très édifiant! Alors quelles solutions s'offrent à nous pour résoudre ces problèmes ? En fait la réponse la plus simple et la plus immédiate, c'est le chiffrement; il peut résider **en plusieurs points de l'infrastructure**. Les puristes diront qu'il faut « encrypter » ou « chiffrer » au plus près de la génération de la donnée. Parmi les options possibles, citons le chiffrement par l'agent de sauvegarde sur le poste où résident les données, le flux de données transite ensuite, en étant crypté, sur le réseau vers le site central et la librairie. Le second modèle s'oriente vers un mode où seul le serveur, responsable de l'écriture des médias, se charge de chiffrer les données et de les inscrire sur le média. La troisième parade, l'un des plus récentes, notamment préconisée par Decru et Neoscale, permet de « chiffrer » les données dans le réseau de stockage, ce qui garantit une donnée chiffrée quel que soit le support (bande magnétique ou disque). Une quatrième option consiste à chiffrer les données dans l'application elle-même, autre que celle chargée d'effectuer le 'backup'. Une bonne référence à mentionner ici est Vormetric. Nous pouvons également citer le système de fichiers chiffré proposé par Microsoft ou d'autres. Car l'offre est très nourrie. Le résultat? Ce doit être, de toutes les façons, **l'écriture de données chiffrées sur le média**. Ainsi l'externalisation peut se dérouler sans crainte car même en cas de perte ou de vol, les informations sont irrécupérables donc inexploitables. Alors optez et optons tous pour ce moyen de garantir l'immunité à nos données. Terminons ce tour d'horizon par un fait très édifiant: les récentes décisions prises par la Morgan Stanley, la célèbre banque d'affaires américaine. Suite à de multiples déboires, comme la perte de bandes de sauvegarde et, en conséquence, des amendes colossales, elle a décidé d'arrêter les sauvegardes sur bandes pour conserver toutes les informations sur disque, pour des besoins de sauvegarde ou d'archivage. Encore une illustration flagrante, si besoin était, de l'actuelle rupture technologique vécue par le marché. (*)*Président et fondateur SNIA France*