

Extrait du Spyworld Actu

<http://spyworld.spyworld-actu.com/spip.php?article5915>

Marc Jourlait (Seagate) : « Demain tous les disques durs seront cryptés »

- Informatique - Sécurité Informatique -



Date de mise en ligne : jeudi 18 octobre 2007

Spyworld Actu

Le constructeur a annoncé lundi une initiative pour standardiser les outils de cryptage des centres de données. Les explications de Marc Jourlait, vice-président chargé du marketing.

01net. : Pourquoi travaillez-vous sur la standardisation des outils de cryptage avec IBM et LSI ?

Marc Jourlait : Nous voulons étendre notre technologie de cryptage FDE (Full Disk Encryption) aux datacenters. Mais pour y parvenir, il faut absolument créer des standards interopérables avec un maximum de matériels de stockage car les centres de données utilisent des solutions de différents fournisseurs. Un point essentiel est de gérer les clés de chiffrement de tous les matériels de manière centralisée. IBM apporte ici son outil logiciel de gestion de clés de chiffrement pour le stockage sur bande. LSI intègre quant à lui nos disques Seagate FDE dans ses baies de disques montées en Raid. Il nous aide aussi à vérifier que le cryptage fonctionne pour l'ensemble de la solution. Nos travaux sont soutenus par le Trusted Computing Group (1) et l'organisme international IEEE (2).

Mais quel est l'intérêt du cryptage en temps réel pour les datacenters qui sont des centres fermés a priori bien protégés ?

Des données très confidentielles peuvent facilement être récupérées lorsque les disques durs arrivent en fin de vie. Actuellement, les techniques d'élimination des disques durs (effacement par réécriture, par aimantation, pilonnage, etc.) sont coûteuses et les procédures de recyclage n'offrent aucune garantie contre la fuite de données. Un disque crypté peut être envoyé au rebut sans crainte car il reste illisible. Demain, toutes les données des datacenters seront cryptées.

Pourquoi ne pas utiliser une solution 100 % logicielle qui permettrait de gérer tous les disques durs quel que soit le fabricant des disques ?

Les solutions de cryptage purement logicielles sont trop lentes car elles sollicitent les ressources processeurs des PC ou des serveurs. L'intégration du cryptage dans le disque dur est la solution la plus performante : chaque disque possède un processeur de cryptage adapté à sa bande passante. En outre, elle est plus facile à administrer. Lorsqu'on ajoute de nouveaux disques, il n'est pas nécessaire d'augmenter la puissance des serveurs chargés du cryptage comme c'est le cas avec les solutions logicielles. Enfin, l'intégration des clés de chiffrement - qui sont elles-mêmes cryptées - dans le disque dur rend le système plus sûr que les solutions logicielles.

Le cryptage est cher. Vos solutions ne risquent-elles pas d'être cantonnées à certaines applications critiques ?

Notre technologie n'est pas très coûteuse. C'est un coût fixe indépendant de la capacité du disque. Pour un client qui achète un PC portable avec disque dur crypté, il faut compter entre 50 et 100 dollars de surcoût. C'est très peu au regard des millions de dollars de pertes que peut générer le vol de données. Néanmoins, dans un premier temps, les responsables informatiques devraient déployer ces technologies pour des besoins spécifiques. Mais ensuite, le cryptage devrait se généraliser, car le fait de différencier les contenus à traiter des autres coûtera plus cher que de tout crypter. En outre, avec l'augmentation des volumes de vente, les prix des disques durs cryptés vont rapidement chuter.

(1) Le Trusted Computing Group est un consortium d'industriels chargé de développer des standards de sécurité.

(2) Le groupe de travail IEEE 1619.3 travaille à la création d'un protocole de sécurité standard permettant de gérer de manière unifiée les clés de cryptage.

Post-scriptum :

<http://www.01net.com/editorial/3626...>-demain-tous-les-disques-durs-seront-cryptes-/