



Article technique

Technologie DriveTrust™ de Seagate : pour la mise en conformité des entreprises avec la législation sur le chiffrement des données

Introduction

Avec l'utilisation croissante des informations numériques, les vols de données et les failles de sécurité informatique font de plus en plus la une de l'actualité. Il semble que chaque semaine apporte son lot de nouveaux cas d'entreprises ou d'autres organisations ayant perdu les informations sensibles d'un client ou d'un employé.

Un cas bien connu est celui du Département des Anciens combattants américains qui a révélé que le PC portable et le disque dur externe, contenant les noms, les numéros de sécurité sociale et les dates de naissance de plus de 26 millions d'anciens combattants, avaient été dérobés chez un analyste informatique. En réponse, la Maison Blanche a demandé un fonds d'urgence de 160 millions de dollars pour financer la surveillance des comptes bancaires des victimes. Plusieurs actions collectives en justice ont été intentées en faveur des anciens combattants, réclamant des millions de dollars de dommages et intérêts.

Il ne s'agissait pas d'un incident isolé. Plusieurs organismes gouvernementaux, institutions financières, compagnies d'assurance, et organisations des domaines de la santé et de l'éducation ont connu des failles de sécurité dans leurs systèmes de données et fait les frais de leur médiatisation. Plus que jamais, les organisations sont mises au pilori lorsqu'elles perdent ou se font voler des informations sensibles.

Pourquoi les constats de vols d'informations sont-ils devenus plus fréquents ces dernières années ? Il existe deux raisons à ce phénomène. Tout d'abord, les travailleurs sont plus mobiles et les entreprises ont de plus en plus de mal à gérer et à protéger les données sensibles se trouvant sur les PC portables et autres appareils mobiles. Les améliorations en matière de technologie d'enregistrement des disques durs ont permis le transport de quantités massives de données sur les PC portables, les téléphones mobiles et les PDA. Ensuite, afin de protéger les informations privées, les législateurs fédéraux et locaux américains ont créé une législation stricte. Celle-ci impose qu'une faille de sécurité soit rendue publique dès lors que les informations n'ont pas été chiffrées. Il est très probable qu'avant cette loi, les violations de données étaient gardées sous silence. Dorénavant, les entreprises sont dans l'obligation d'effectuer des rapports publics.

Technologie DriveTrust de Seagate : pour la mise en conformité des entreprises avec la législation sur le chiffrement des données



Législation sur le chiffrement des données

Cette législation oblige les organisations de toute taille à protéger leurs informations sensibles. En juillet 2003, la Californie devenait le premier État à édicter une loi obligeant à protéger les données numériques sensibles et, pour les organisations victimes de vols de données non chiffrées, à informer toute personne dont les informations personnelles ont été compromises.

En septembre 2006, 29 autres États lui emboîtaient le pas en édictant leur propre législation sur la confidentialité des données. Dans la majorité des cas, les entreprises qui ne respectent pas la loi sont sanctionnées par des amendes lourdes et la notification publique de la faille.

Le gouvernement des États-Unis n'a pas ignoré l'importance du chiffrement des données et le Congrès prévoit plus de 20 projets de loi portant sur ce sujet. Les plus importants sont les suivants :

- Amendment to the Fair Credit Reporting Act (HR 3997)
- Data Accountability and Trust Act (HR 4127)
- Cyber-Security Enhancement and Consumer Data Protection Act of 2006 (HR 5318)
- Federal Agency Data Privacy Protection Act (HR 5820).

À l'instar des lois sur le chiffrement des données désormais en vigueur dans les États, les projets de loi fédéraux ont exclu les données chiffrées de ces dispositions. En revanche, si les informations n'ont pas été chiffrées et qu'une faille de sécurité se produit, l'entreprise doit le signaler publiquement et payer de lourdes amendes. La loi HR 5318 prévoit même des sanctions pénales.

En plus des réglementations gouvernementales, l'industrie des cartes de crédit a établi ses propres conditions de sécurité, y compris l'autorisation de chiffrer les données.¹

Le prix à payer pour les données non chiffrées

Une faille de sécurité sur des données non chiffrées peut coûter très cher. Les experts estiment que le coût d'une seule faille de sécurité s'élève à environ 14 millions de dollars en coûts directs (tels que les frais de justice ou la notification aux clients), en coûts indirects (perte de productivité) et en manque à gagner (perte de clients et de prospects).

De nombreuses entreprises en ont directement fait les frais. Par exemple, en 2005, une entreprise de collecte de données a divulgué par inadvertance les informations confidentielles de quelque 145 000 clients à des escrocs. Elle s'est donc vue dans l'obligation de payer 11,4 millions de dollars de dommages et intérêts et 15 millions de dollars d'amende à la Commission fédérale du Commerce américaine (Federal Trade Commission). Elle a, de plus, perdu 20 % de ses clients.

Avec plusieurs millions de dollars et leur réputation commerciale en jeu, les organisations ont réellement besoin d'une solution capable de préserver la confidentialité des informations et de s'assurer que ces données restent protégées en cas de vol. Le chiffrement est non seulement cité dans la législation, il est également reconnu par les experts en sécurité comme la meilleure méthode de sécurisation des données.

Plusieurs options de chiffrement des données sont proposées aux entreprises. L'une d'elle est le chiffrement logiciel. Par exemple, certaines applications offrent la possibilité de chiffrer les fichiers, les dossiers, les partitions ou même les disques. Mais cette méthode de chiffrement reste limitée.

Le chiffrement des fichiers et des dossiers s'applique à des fichiers ou des répertoires spécifiques, ce qui oblige l'utilisateur à gérer lui-même la sécurité des données. S'il n'a pas sélectionné ou stocké les informations sensibles dans le répertoire approprié, ces données ne sont pas chiffrées.

Le chiffrement logiciel d'une partition ou d'un disque est vulnérable aux erreurs et aux bogues logiciels, aux programmes malveillants ou aux failles de sécurité du système d'exploitation. De plus, un échec ou la corruption du code de chiffrement peut rendre l'ensemble de la partition ou du disque inutilisable.

Le chiffrement logiciel est une application intensive qui sollicite d'importantes ressources au niveau de la mémoire et du processeur. Les entreprises doivent donc faire un compromis entre la sécurité et les performances du système.

Aujourd'hui, Seagate®, premier fabricant mondial de disques durs et précurseur en matière de technologie de stockage, innove avec la technologie DriveTrust™. Cette technologie déploie le chiffrement là où se trouvent les données : sur le disque dur. La technologie DriveTrust permet, de manière très simple, de déployer une sécurité renforcée sans affecter les performances du système.

¹ Pour plus d'informations, voir le site http://www.vigilantminds.com/sols_spci.php.

Technologie DriveTrust de Seagate : pour la mise en conformité des entreprises avec la législation sur le chiffrement des données



Un chiffrement novateur pour une sécurité des données optimale

La technologie DriveTrust est une plate-forme de sécurité matérielle du disque qui exploite le fait que le disque dur est isolé du reste du système informatique. Contrairement aux environnements de systèmes d'exploitation, conçus pour permettre la prise en charge d'applications étendues, les disques durs constituent des environnements informatiques protégés exécutant des codes spécifiques pour la gestion des fonctions du disque. Ainsi, le disque dur s'impose comme l'emplacement idéal pour l'implémentation d'une sécurité des données, car ses opérations internes sont inaccessibles aux autres éléments du système informatique.

La technologie DriveTrust fait appel à une authentification et un chiffrement renforcés au sein même du disque dur afin de constituer une base sécurisée et conforme avec la législation relative à la sécurité et à la confidentialité des données. Le disque pour PC portables Seagate Momentus® 5400 FDE.2 est le premier disque dur doté d'un chiffrement intégral. Les disques Momentus de 2,5 pouces et 5 400 tr/min constituent un moyen simple et rentable de protéger l'ensemble des données des PC portables contre tout accès non autorisé, que le système ou le disque soit perdu, volé, recyclé ou revendu.

Le chiffrement matériel complet du disque dur offre une protection beaucoup plus sûre que les approches de chiffrement traditionnelles, car les opérations de chiffrement et le contrôle d'accès s'effectuent en toute sécurité à l'intérieur même du disque dur. Les utilisateurs ont juste besoin d'un mot de passe d'authentification permettant l'accès complet au disque, alors que la sécurité des tiers est renforcée avec la possibilité d'une authentification multiple par empreinte digitale et carte à puce. De plus, l'initialisation et la configuration d'avant déploiement du disque sont rapides.

Technologie DriveTrust : la sécurité des données simplifiée

Pour certaines organisations, le déploiement et la maintenance de la technologie de chiffrement des données sont trop complexes et coûteux. De nombreuses solutions de chiffrement réduisent la productivité de l'utilisateur, ralentissent les performances du système ou offrent des fonctions de chiffrement très limitées. La technologie DriveTrust constitue un moyen de chiffrement des données simple, rentable, mais aussi puissant.

Les avantages de la technologie DriveTrust sont multiples :

- **Sécurité permanente** : de nombreuses solutions de chiffrement des données sont difficiles à utiliser, car il faut constamment configurer et gérer la sécurité. Les employés contournent le problème en désactivant tout simplement la technologie de chiffrement, ce qui augmente le risque de non conformité de l'organisation. La technologie DriveTrust offre un chiffrement et une sécurité intégrés, transparents et permanents.
- **Hautes performances** : les disques durs dotés de la technologie DriveTrust intègrent une puce conçue pour chiffrer et déchiffrer efficacement l'ensemble des données stockées sur le disque, sans affecter les performances du système.
- **Facilité de déploiement** : grâce à la technologie DriveTrust, l'installation et le fonctionnement des disques durs sont aussi simples que pour des disques standard. Les fonctions de sécurité sont exécutées de façon transparente, à l'intérieur même du disque, et ne nécessitent aucune configuration supplémentaire. La configuration peut être très simple puisqu'il suffit de créer un mot de passe pour activer une clé de chiffrement.
- **Maintenance minimale** : la sécurité du disque ne nécessite aucun patch, mise à jour ou mise à niveau, d'où la suppression des coûts associés aux solutions logicielles. Grâce aux disques durs DriveTrust, les organisations informatiques n'ont plus à fournir de mises à jour ni à gérer les différentes versions logicielles, garantissant ainsi une sécurité uniforme et fiable pour les données au repos.
- **Effacement sécurisé** : les informations stockées sur les disques durs DriveTrust peuvent être effacées instantanément, ce qui facilite le redéploiement ou le recyclage des disques et réduit le temps et le coût généralement associés à l'écrasement ou à l'effacement des données.

Conclusion

Les enjeux sont de taille. Les organisations doivent trouver le moyen de chiffrer les données confidentielles sur des appareils fixes et mobiles sous peine de devoir payer de lourdes amendes ou de subir la publicité négative qui peut résulter d'un vol de leurs données. Le chiffrement est reconnu par la législation comme étant la meilleure méthode de protection des données. La technologie DriveTrust offre un chiffrement des disques complet et performant qui brouille

Technologie DriveTrust de Seagate : pour la mise en conformité des entreprises avec la législation sur le chiffrement des données



les données et les protège des accès non autorisés sur les PC portables, appareils électroniques grand public ou tout autre équipement informatique disposant d'un disque dur. Les disques durs DriveTrust proposent la méthode de chiffrement la plus transparente, la plus fiable et la plus rentable qui soit.

Ressources

Pour plus d'informations sur la technologie DriveTrust :

- Consultez le site Web www.seagate.com/newsinfo/technology/drivetrust/index.html.
 - Lisez l'article technique de présentation de la technologie DriveTrust du point de vue managérial.
 - Lisez l'article de présentation technique de la technologie DriveTrust.

AMÉRIQUES Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIE/PACIFIQUE Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MOYEN-ORIENT ET AFRIQUE Seagate Technology SAS 130-136, rue de Sully, 92773, Boulogne-Billancourt Cedex, France, 33 1-41 86 10 00

Copyright © 2006 Seagate Technology LLC. Tous droits réservés. Imprimé aux USA. Seagate, Seagate Technology et le logo Wave sont des marques déposées de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. DriveTrust et Momentum sont des marques ou des marques déposées de Seagate Technology LLC ou de l'une de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques ou marques déposées appartiennent à leurs propriétaires respectifs. Un gigaoctet (ou « Go »), en termes de capacité de disque dur, équivaut à un milliard d'octets. Seagate se réserve le droit de modifier sans préavis les offres ou les caractéristiques de ses produits. Numéro de publication : TP566, novembre 2006