

eCLIPse
Systeme de sécurité aux entreprises



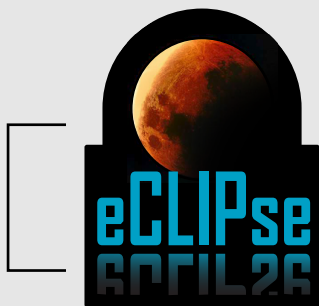
IT Business and Marketing Solutions Inc.

6710, Sherbrooke Est, bureau 200 Montréal, Québec H1N 1C9

Téléphone: +1 514-764-0133

www.itbms.biz

Email: sales@itbms.biz



eCLIPse **Systeme de sécurité aux entreprises**

Introduction

Depuis quelques années, nous assistons à une augmentation croissante des coûts reliés à la perte ou au vol d'ordinateurs contenant des données confidentielles. Ces appareils renferment des informations confidentielles et dans certains cas, irremplaçables. Par ailleurs, des attaques informatiques ont permis à des pirates (hackers) d'accéder à des bases de données contenant des informations confidentielles telles que le nom des clients, leur numéro de compte, d'hypothèque ou de carte de crédit, etc.

Ces événements ont amené les institutions (bancaires, de prêt, de crédit, financières, gouvernements, etc.) à prendre des mesures de sécurité de plus en plus importantes. Cette situation résulte en une augmentation constante des frais d'exploitation reliés à la sécurité.

À titre d'exemple, nous pouvons citer le dépassement des coûts associés à l'émission de nouvelles cartes de crédit, à la création de nouveaux numéros de comptes bancaires ainsi que les campagnes de sensibilisation visant à informer et à conseiller les déposants ou les créanciers touchés par les changements et celles qui ont pour but d'éviter les fraudes internes et de scruter la responsabilité de l'institution à l'égard des pertes.

Ces risques concernent également les entreprises, les cabinets d'avocats, le milieu médical, les assureurs, l'armée et les gouvernements. Il incombe de nos jours aux entreprises et aux institutions publiques de protéger le caractère confidentiel des dossiers et des archives électroniques qu'elles stockent dans des ordinateurs portables ou dans leurs réseaux. « S'il revient au canal de communication de protéger l'intégralité des données pendant leur transfert, le dossier reçu ne doit pas pour autant être transmis ou stocké dans l'ordinateur dans un format lisible ».

Aux fins de protection des données, l'expéditeur a l'obligation de créer et de transmettre au récepteur un dossier encrypté que le récepteur pourra décrypter. En outre, les administrateurs de bases de données doivent s'assurer que l'information confidentielle est encryptée de façon sécuritaire. Il convient de remarquer que les logiciels antivirus ne sont pas toujours efficaces contre une classe de programmes malveillants communément appelés logiciels-espions (spyware), certains s'introduisent dans l'ordinateur de l'utilisateur, observent avec précaution les archives que ce dernier manipule pendant une session de travail et transmettent furtivement ces archives au système informatique répréhensible. Ce risque est toujours présent quand les données confidentielles sont stockées sans être encryptées.

Rôle et importance de l'encryptage des données

Dans la Grèce antique, on tuait les messagers afin de se saisir des messages cryptés et d'éviter de la sorte qu'ils soient lus par l'ennemi. Dans les endroits peu sécuritaires, l'encryptage par l'expéditeur et le décryptage par le récepteur sont essentiels pour protéger leur contenu. De nos jours, il existe plusieurs méthodes pour assurer la sécurité des données. La première exige d'encrypter le disque dur en entier, la deuxième, d'encrypter uniquement les fichiers de données et la troisième, d'encrypter à la fois les archives contenant les données et le disque dur.

Encryptage complet du disque dur

La section suivante provient de l'encyclopédie libre Wikipedia.

Si on le compare avec l'encryptage du « dossier normal », avec « l'encryptage du fichier » ou avec « Le l'encryptage du coffre-fort », l'encryptage complet du disque dur présente les avantages et les désavantages suivants :