CHIFFREMENT DES DONNEES STOCKEES

Définition

Le chiffrement des données est l'opération qui consiste à transformer à l'aide d'un calcul algorithmique, les informations en clair, en informations incompréhensibles sans la connaissance d'un secret.

Algorithme de chiffrement

Pour chiffrer des informations volumineuses, ce qui généralement est le cas des données stockées, on utilise des algorithmes dits « symétriques », qui mettent en œuvre le même secret pour les opérations de chiffrement et de déchiffrement. En dehors des domaines étatiques, ce sont généralement des algorithmes publiés comme le DES, ou l'AES qui sont utilisés ; l'AES est le standard international depuis quelques années.

Les algorithmes asymétriques, peuvent intervenir dans le schéma de sécurité, par exemple pour le chiffrement de clés symétriques ; l'algorithme asymétrique le plus connu est le RSA qui met en œuvre un bi-clé comportant une partie publique (pour le chiffrement) et une partie secrète (pour le déchiffrement). Cette famille d'algorithme, plus lourde en temps de calcul, n'est pas utilisée pour le chiffrement direct des données.

Un algorithme est d'autant plus puissant que sa clé est longue ; l'ANSSI recommande une taille minimale de 128 bits pour les clés symétriques (les solutions du commerce utilisent généralement des clés de 256 bits) et de 1536 bits pour les clés asymétriques.

Importance du schéma de sécurité

Les procédures de génération des clés, les moyens mis en œuvre pour les stocker et garantir leur confidentialité, etc… sont des éléments majeurs, qui contribuent à la solidité de la solution de chiffrement et à son niveau fonctionnel.

Cas d'application ou d'usage du chiffrement des données

Le cas d'usage les plus répandu est la protection contre la perte ou le vol d'un équipement portable : poste de travail, support USB, Smartphone, etc….. Le propriétaire de l'équipement étant le seul à détenir la clé de chiffrement (mot de passe, Token, Carte à puce) la confidentialité des données reste assurée, elles ne pourront être lues par un tiers.

Un autre cas d'usage important est possible avec un schéma de sécurité élaboré : le chiffrement permet de gérer le "droit d'en connaitre", c'est-à-dire cloisonner les données entre utilisateurs ou groupes d'utilisateurs ; Seules les personnes autorisées pourront consommer les données ; ce cas d'usage est important pour gérer les partages sur les serveurs de données ou sur les portails de travail collaboratifs tels que SharePoint par exemple.

Procédés

Les procédés de chiffrement des supports de données utilisent des moyens matériels (disques chiffrant par exemple) ou logiciels (les plus répandus). On utilise également des moyens mixtes où un logiciel de chiffrement est associé à une clé protégée par un moyen matériel (carte à puce ou token USB). Avec les procédés actuels, les opérations de chiffrement/déchiffrement sont devenues quasi transparentes pour les utilisateurs et impactent peu les performances des ordinateurs.

Exemples

La protection de la confidentialité des données est devenue une problématique complexe et critique pour les entreprises. Toutes sortes d'informations confidentielles (techniques, commerciales, personnelles …) sont éparpillées sur toutes sortes de supports de données : postes de travail des utilisateurs dans l'entreprise mais également ordinateurs et téléphone portables circulant à l'extérieur de l'entreprise tout comme les supports amovibles souvent de petites tailles et facilement égarables par les utilisateurs.

Face à cela, le chiffrement adresse toute la problématique d'accès non autorisé aux données :

- Chiffrement des serveurs et des postes de travail pour lutter contre les tentatives d'intrusion interne ou externe (locales ou en réseau).
- Chiffrement des téléphones portables, des tablettes tactiles, des ordinateurs portables et des supports amovibles (particulièrement les clés USB) pour contrer le vol ou la perte accidentelle de ceux-ci. Le dommage est alors ramené au coût du support perdu (si, en parallèle, des mesures ont été préalablement prises contre la perte de leur disponibilité).

Cibles

Toutes les entreprises, quelques soient leur taille et leur domaine d'activité, sont concernées par le chiffrement dans la mesure où elles sont exposées au vol ou à la perte de leurs données confidentielles à l'intérieur et à l'extérieur de leur enceinte : savoir-faire, fichier client, informations sur les salariés … Les outils de chiffrement de données utilisateur voient leur niveau de déploiement augmenter peu à peu avec 40% des entreprises qui étaient équipées fin 2010 (source Clusif). Les ordinateurs portables restent les plus concernés par cette mesure mais le taux d'équipement reste malgré tout relativement faible au regard des parcs de portable en circulation.

L'Administration utilise des moyens de chiffrement avec des besoins très différents selon les secteurs. Traditionnellement, en raison de la sensibilité des informations manipulées, les milieux militaires et gouvernementaux ont été les premiers à mettre en œuvre les procédés de chiffrement.

Le marché des particuliers est peu important, ceux-ci utilisent la plupart du temps des solutions open source.

Cadre réglementaire

En vertu de l'article 30 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, l'utilisation des moyens de cryptologie est libre en France. En revanche, la fourniture, le transfert depuis ou vers un Etat membre de la Communauté européenne, l'importation et l'exportation de ces moyens sont réglementés lorsque ces moyens n'assurent pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité. Ces opérations sont en général soumises au régime de la déclaration.

Evaluation des risques

Les principaux moteurs du marché du chiffrement dans le monde sont la protection des données confidentielles ou nominatives, la prévention de la perte de réputation, et surtout la protection de la responsabilité pénale du dirigeant. Certains types d'informations sont protégés par des lois nationales, d'autres par des réglementations locales ou par des conventions professionnelles.

La divulgation d'informations confidentielle peut exposer une entreprise à de lourdes amendes, voire à des poursuites judiciaires, selon les efforts déployés au niveau des mesures de sécurité préventives. Concernant le traitement des données à caractère personnel, l'entreprise est soumise à des obligations de mise en œuvre de moyen de protection au titre de l'article 34 de la Loi Informatique et Libertés, « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Le non respect de ces obligations peut entraîner de lourdes sanctions. Par ailleurs la révision en cours de la directive européenne en matière de protection des données à caractère personnel va amener un renforcement de la législation. En particulier tout vol de données personnelles non chiffrées devra être notifié aux personnes concernées.

Les exemples de pertes de données à caractère personnel pullulent dans la presse, l'un des plus célèbres a eu lieu en Grande-Bretagne où 600 000 personnes ont vus leurs données personnelles disparaître lors du vol de l'ordinateur portable d'un officier de la Marine. Le dossier contenait des informations très sensibles de personnes voulant rejoindre la Marine avec des numéros de passeports, de sécurité sociale, de permis de conduire et autres renseignements familiaux et bancaires.

Les coûts directs et indirects entraînés par une faille de sécurité peuvent également inclure la perte de savoir faire, de clients ainsi que la dépréciation de la crédibilité et de la réputation de l'entreprise. En avril 2011, des pirates ont volé les données personnelles de plusieurs dizaines de millions d'utilisateurs du Playstation Network de Sony. Sony a par ailleurs reconnu que, lors de cette intrusion, les informations bancaires de plusieurs millions de personnes ont pu être dérobées. Le préjudice estimé par Sony s'élève à 120 millions d'euros. Plus récemment, un grand groupe français a été victime d'une intrusion de grande ampleur qui a durée 2 ans et l'a contraint à renforcer la sécurité de ses réseaux. Dans tous les cas, une fois les barrières traditionnelles franchies, seul le chiffrement permet aux données « de se défendre ».

Moyens de protection

Certains disques durs intègrent des algorithmes de chiffrement reposant sur le standard défini par le Trusted Computing Group. L'intérêt principal de ces prochaines générations de périphériques de stockage « self-encrypted », c'est que le système de chiffrement est intégré sur une puce dans le disque. Par contre ces solutions ne sont pas administrables à grande échelle (ils ne proposent pas de clés de recouvrement par exemple).

Les éditeurs de logiciel proposent aujourd'hui des solutions de chiffrement. Les offres sont nombreuses en ce qui concerne la protection des postes de travail portable (chiffrement du disque dur) et des supports USB. Quelques éditeurs proposent des solutions élaborées permettant de gérer le droit d'en connaitre sur les serveurs de données et les portails de travail collaboratif.

Liens utiles

Pour plus d'informations, se référer à la documentation disponible sur le sujet, et notamment les liens Internet suivants :

Réglementation française en matière de cryptologie :
http://www.ssi.gouv.fr/fr/reglementation-ssi/cryptologie/

Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques :
http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf