Logique de Sécurité des Systèmes d'Information

par Aymeric MORILLEAU

Date de publication : 08/03/05

Dernière mise à jour : 08/03/05

Comment efficacement protéger ses données de la divulgation et de l'altération ? Importante question dés lors que l'utilisation des systèmes informatiques implique la génération de données importantes et/ou confidentielles !

1 - Notions de base

1-A - Introduction

Chaque société dispose aujourd'hui d'un volume non négligeable d'informations aux formats informatiques, ces données sont souvent d'une importance cruciale dans la survie de l'entreprise. Il est donc important de protéger ces informations, aussi bien de la divulgation, que de l'altération.

La SSI, est la Sécurité des Systèmes d'Information, elle doit être au centre de toute société voulant préserver ses travaux, ses secrets, ses avantages concurrentiels, ...

Pour obtenir le résultat escompté, les moyens sont :

- la classification de l'information
- le choix des mots de passe
- la protection du poste de travail
- la cryptographie
- la sauvegarde

Cette article ne traitera bien sûr que de la SSI appliquée à l'informatique, la SSI couvrant un domaine bien plus important, concernant le recrutement, la sécurité des locaux, la sécurité des informations aux formats papiers #

1-B - Classification des informations

Pour être efficace dans la mise en place d'une SSI, il faut savoir quels documents méritent ou non une protection. En effet il vaut mieux chercher à sécuriser une zone restreinte mais de manière optimale plutôt que de chercher à tout sécuriser, ce qui impliquerait à coup sûr des failles de sécurité importantes.

Il faut donc classer l'information, la classification selon 3 étages dans lesquels ont peut placer les documents :

- « **à diffusion contrôlée** » : Ces documents n'ont pas une importance primordiale, leur diffusion n'entraînera qu'une perturbation ponctuelle pour l'entreprise. On peut parler de préjudice faible.

- « **confidentiel** » : Ces documents ont une importance non discutable, leur diffusion entraînera des séquelles compromettant l'action à court et moyen terme. On peut parler de préjudice grave.

- « **secret** » : Ces documents ont une importance centrale et irréprochable, leur diffusion entraînera des séquelles graves et durables. On peut parler de préjudice inacceptable.

Cette classification, permet à la personne qui a le document en sa possession de se rendre compte de son importance et de l'attention à lui porter. Cette classification permet également de savoir quel protocole de sécurité appliquer au document.

1-C - Choix des mots de passe

Dans une logique de SSI, beaucoup de mots de passe sont amenés à intervenir, leur choix et leur « entretien » sont donc importants, en effet quel est l'intérêt de baser une logique de sécurité sur un mot de passe qui n'est pas optimal.

Il est conseillé de choisir des mots de passe d'au moins 8 caractères alphanumériques. Et si possible en utilisant plusieurs casses (minuscules et majuscules). En effet le mot de passe « **A23df4tg** » sera beaucoup plus difficile à casser que « **voitures** ». Cependant un mot de passe doit aussi être facilement mémorisable, on peut donc intervertir nom et date, par exemple : M. **J**ean-**C**laude **Du**rand né en *1965* pourrait choisir « *1***J***9***C***6***Du***5** », on obtient un mot de passe alphanumérique facilement mémorisable.

Un mot de passe ne doit pas être statique, en fonction de son importance dans la logique de SSI, il doit être changé de manière régulière. Cependant il est plus important d'avoir en place des mots de passe difficilement cassables, plutôt que des mots de passe très dynamiques : en effet il vaut mieux garder quelques mois un mot de passe alphanumérique de 8 caractères, plutôt que de mettre le prénom des membres de sa famille en les changeant toutes les semaines !

ATTENTION : Ne jamais mettre en place de protocole de création de mot de passe, car si ce protocole est découvert, tous les mots de passe générés deviennent vulnérables, et donc les informations qu'ils protégent aussi.

Pour vous assiter dans l'administration des mots de passe, Windows (dans ses version 2000 et XP Pro) propose une option qui s'appelle ***"Les mots de passe doivent respecter des exigences de complexité"*** Cette option implique que les mots de passe doivent alors avoir au moins 8 caractères, une majuscule, un chiffre, un caractère spécial.

Cette option se trouve dans :

Panneau de configuration -> outils d'administration -> stratégie de sécurité locale -> Stratègie de comptes -> Stratégie de mot de passe

2 - Protection du poste de travail

2-A - Mot de passe BOOT

Le mot de passe BOOT peut paraître simpliste, mais il a une importance non négligeable, en effet il empêche le BOOT (comme son nom l'indique, il est aussi appelé « Mot de passe BIOS » par abus de langage).

Il est en effet très intéressant de bloquer le BOOT, car une personne malveillante qui ne disposerait pas des mots de passe placés au log sous Windows pourrait très bien booter sur un live CD (type Knoppix / Windows PE / Bizantine) et accéder à la plupart des données du poste.

Le mot de passe BOOT est paramétrable depuis le BIOS de la carte mère, chaque BIOS étant très différent suivant les fabricants de carte mère, il n'existe pas de protocole universel, cependant la lecture de la documentation de la carte mère vous donnera toutes les informations nécessaires.

2-B - Mot de passe administrateur

Lors de l'installation de Windows, un mot de passe dit « administrateur » est fixé, ce dernier permet de se logger en tant que « super utilisateur » sur le poste, pour administrer un grand nombre de paramètres, incluant la modification des comptes utilisateurs et de leurs mots de passe.

Il faut être vigilant lors de l'achat de PC livré avec l'installation de Windows comprise. Dans ce cas si la personne qui a installé Windows n'a pas fixé un mot de passe administrateur, le compte « super administrateur » a pour login : « administrateur » mot de passe : « {vide} ». Une personne malveillante peut donc facilement se logger en « super administrateur » et accéder à toutes les informations du poste de travail.

Il faut donc à la réception de ces machines (PC livré avec Windows pré installé), se logger en « super administrateur », puis modifier le mot de passe de cette session.

2-C - Protection individuelle

Une administration convenable du poste est nécessaire, il faut en effet mettre à jour régulièrement Windows et ses programmes afin de refermer les failles régulièrement repérées#

Je vous renvoie sur le très bon article de **cchatelain** traitant du sujet :

Article de cchatelain sur la protection individuelle

Il est également très important de se prévenir des spywares, trojans, virus... Une solution gratuite : l'utilisation des quatre logiciels : SpybotSD, Ad-AwarePersonal, AVast et SygatePersonalFirewall.

2-C-a - Coupler les logiciels Spybot SD et Ad-Aware SE

Logiciel Spybot SD (Search and Destroy)

http://www.spybot.info/fr/index.html

Logiciel Ad-Aware SE Personal

http://www.lavasoft.com/

ATTENTION : Tout comme les antivirus, les anti-spyware fonctionnent sur une liste de spyware reconnu, cette liste doit être régulièrement mise à jour pour garantir une protection optimale.

2-C-b - Logiciel Antivir

www.free-av.com

La maintenance, les mises à jour et le programme sont gratuits.

ATTENTION : Dans la majorité des cas, l'antivirus n'est disponible que quelques temps (semaine / mois) après l'apparition du virus lui-même, un antivirus ne dispense pas des règles primaires de maintien du système.

2-C-c - Logiciel Sygate Personal Firewall

http://www.sygate.com/firewall/

2-D - Authentification forte

Si l'utilisation de mots de passe vous paraît faible face à l'importance des données en jeux l'authentification forte peut être envisagée. Elle consiste en la nécessité d'un élément physique pour le log (token #clé usb#, carte à puce, biométrie) en plus d'un mot de passe ou d'un code PIN.

Les tokens sont de petites clés USB de quelques Ko.

3 - Cryptographie

3-A - Introduction

La cryptographie est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information telles la confidentialité, l'intégrité des données, l'authentification d'entités, et l'authentification de l'originalité des données. C'est un ensemble de techniques qui fournit la sécurité de l'information.

La cryptographie est la réponse au besoin d'impossibilité de divulgation des données.

3-B - Notions de base

Il existe deux grandes techniques de cryptographie : les systèmes de cryptographie à clés asymétriques et ceux à clés symétriques.

La cryptographie à clés symétriques est la plus connu, le document est chiffré avec une certaine clé, et il faut cette même clé pour déchiffrer le document.

La cryptographie à clés asymétriques se base sur le principe d'une clé dite publique, que l'on peut divulguer, qui permet de chiffrer le document par l'émetteur, et d'une clé dite privée, secrète, qui permet au destinataire de déchiffrer le document.

La cryptographie a deux applications : l'authentification de l'auteur des documents, le stockage sécurisé de données. La seconde utilisation est bien entendu la plus utilisée, mais il ne faut pas négliger la première qui, avec l'utilisation grandissante du mail, va très vite devenir indispensable pour certifier l'authenticité des courriels.

3-C - Solutions gratuites au stockage sécurisé

Il sera présenté ici trois solutions.

- **Cryptographie avec WinRAR**

En effet, le logiciel WinRAR est connu pour la création d'archives. Il permet également de placer des mots de passe sur ces archives, ce qui limite l'utilisation des documents archivés. Cependant le chiffrage par WinRAR est aussi faible qu'il est simple, il convient donc pour des documents ***à diffusion limitée***. (WinRAR est distribué sous licence shareware)

- **Cryptographie avec SecurityBox Freeware**

La société MSI (Site de MSI SA) propose une solution de cryptographie appelée SecurityBox, cette solution inclut une version Freeware (gratuite), de cryptographie. Ce logiciel permet de chiffrer un

document avec l'algorithme 3DES (lisez « triple dèsse ») et une clé de 128 bit. Cette cryptographie à clés symétriques peut être qualifiée de bonne qualité, elle convient pour la protection de document ***confidentiels***.

- **Cryptographie avec PGP Freeware**

Ce programme gratuit permet de mettre en place une logique de cryptographie complète. Il dispose des plug-in suivant :

- Eudora
- Microsoft Exchange/Outlook
- Microsoft Outlook Express
- PGPDisk

Le plug-in PGPDisk présente le grand interet de faire du cryptage de partition a la volée.

La solution FGP freeware est téléchargeable ici

3-D - Solutions payantes

Il existe de nombreuses solutions de cryptographie, lors de votre choix vous devez privilegier la robustesse de l'algorithme, ainsi un 3DES avec des clés d'au moins 512 bit (en fonction de la puissance de votre poste de travail) semble etre un bon compromis.

Sachez qu'il existe également des solutions de cryptage de disque complet dit « à la volée » : ce type de solution permet d'avoir ses données chiffrées en permanence sur son disque, chaque donnée est déchiffrée à la volée lors d'une demande d'accès par un programme.

4 - Sauvegarde

La SSI ne se limite pas à la protection des données face à la divulgation d'éléments stratégiques, elle inclut également la sauvegarde des informations propriétaires.

Il faut distinguer deux types de sauvegarde : les sauvegardes juxtaposées, les sauvegardes autonomes.

4-A - Les sauvegardes incrémentales

Ces sauvegardes couvrent chacune le travail réalisé depuis la précédente, elles doivent être réalisées à intervalles réguliers et rapprochés. On pourrait les appeler « sauvegarde temps réel ».

Ce type de sauvegarde doit être réalisé au minimum une fois par jour, ensuite chaque situation implique sa politique de sauvegarde, suivant le volume d'informations générées, la stabilité des lieux de stockage#

4-B - Les sauvegardes complètes

Ces sauvegardes, ont pour but de pouvoir régénérer l'intégralité du parc informatique en cas d'altération grave des éléments de stockage (vol de serveurs, crash de disque durs#)

Ces sauvegardes doivent être faites plus rarement, un minimum d'une tous les deux semaines me paraît raisonnable, il faut bien sûr adapter ce délai à la situation de l'entreprise suivant les mêmes critères que les sauvegardes incrémentales. Cependant, ces sauvegardes doivent être faites de manière très consciencieuse : la solution parfaite, mais très lourde, étant de conserver un ghost de chaque disque dur du parc informatique. Il faut donc trouver un compromis, entre étendue de la sauvegarde, et réalisme de la mise en #uvre.

4-C - Gestion des sauvegardes

Une sauvegarde doit être testée : en effet, copier des fichiers sur un support amovible (disque externe, DVD, CD, ..) ne suffit pas, il faut être sûr que la sauvegarde permet de remettre dans son état antérieur le parc informatique. Pour cela il faut prendre une sauvegarde complète, la redéployer, puis lui appliquer la sauvegarde incrémentale suivante, afin de retrouver le parc informatique en l'état de la date de réalisation de la sauvegarde juxtaposée appliquée.

4-D - La solution RAID

Le système de gestion de disque RAID permet plusieurs combinaisons. Celle qui nous intéresse est le RAID 0. En effet dans cette configuration, deux disques logiques (respectivement deux disques physiques dans notre cas) sont gérés comme un seul disque et sont en permanence l'image de l'autre, ce qui présente comme intérêt qu'en cas de plantage irrécupérable de l'un des deux disques, le second contient toujours l'intégralité des informations, et permet de continuer à travailler et à générer un nouveau disque pour la remise en place du RAID.

Cette solution permet donc de se protéger des pertes de données dues à des défaillances matérielles.

Pour plus d'info sur le RAID, consulter ce lien :

http://www.axis.fr/produits/tutorial/raid.htm

Attention, le RAID ne dispense pas de faire des sauvegardes sur bande.

5 - Résumé

- Il faut **classer** l'information selon son niveau de confidentialité, pour rester optimal dans la mise en place de la SSI :
- Il faut utiliser des mots de passe **alphanumériques** d'au moins **8 caractères**, qu'il faut changer de manière régulière, mais pas au détriment de la complexité de ce dernier
- Il faut mettre en place un **mot de passe BOOT** sur chaque poste de travail
- Il faut vérifier l'existence du mot de passe « super administrateur » de Windows.
- Il faut respecter une **bonne protection individuelle**, anti-Spyware, anti-Virus, firewall, mise à jour du système d'exploitation et des programmes ayant accès à Internet
- Il faut **chiffrer** les données sensibles
- Il faut mettre en place une politique de **sauvegarde** efficace et fonctionnelle (test de rapatriement des sauvegardes)

6 - Liens utiles

Vous pouvez télécharger ce cours au format PDF ICI

Pour toute information complémentaire consultez les liens suivants