CNRS/FSD/Sécurité des Systèmes d'Information

Recommandations pour la protection des données et le chiffrement

En date du 17 avril 2008
Référence 08.1840/FSD

Nature du document : Recommandations

Destinataires :

- directeurs d'unité
- responsables informatiques
- tous utilisateurs

Mise en œuvre : Ces recommandations sont d'application générale. Il est toutefois souhaitable qu'elles soient explicitement intégrées dans la politique de sécurité des systèmes d'information de l'unité. Cette politique pourra préciser le cas échéant, en fonction des particularités de l'unité, les dérogations possibles à ces recommandations et en contre partie les moyens permettant de viser un niveau acceptable et contrôlé de sécurité.

Version 1.0

Recommandations

Le chiffrement est une technique qui permet d'interdire de prendre connaissance des informations à quiconque ne possède pas la convention pour les déchiffrer. Il est une excellente solution pour protéger des données susceptibles d'être interceptées.

Connexions à distance

Se connecter à distance depuis l'extérieur pour gérer son courrier, ouvrir une session sur un serveur, transférer des fichiers est bien utile mais encore faut-il le faire avec un niveau de sécurité satisfaisant. Un préalable est une authentification fiable. Or très souvent durant la phase d'authentification des connexions à distance, le mot de passe qui doit, par définition, rester secret circule en clair. Certes des mécanismes permettant de protéger spécifiquement cette phase sont bien prévus par les différents protocoles mais ils sont rarement implémentés sur les produits disponibles. Pratiquement cela signifie que pour protéger le mot de passe, il faut chiffrer l'ensemble de la connexion ce qui offre, en outre, la protection contre les écoutes des données échangées.
La règle qui s'impose est de chiffrer systématiquement toutes les connexions à distance. Il existe deux façons de le faire. La première consiste à utiliser des protocoles sécurisés :

- IMAPS, POP3S, SMTPS pour le courrier électronique ;
- SSH pour l'ouverture de sessions à distance ;
- HTTPS pour la connexion sur un Intranet ou la gestion du courrier à l'aide d'un Webmail ;
- SFTP pour le transfert de fichiers.

La seconde fait transiter les connexions dans un tunnel chiffré. On parle alors de réseau privé virtuel (VPN). Parmi les outils disponibles on peut citer : IPSec, OpenVPN, voire SSH.
Il est demandé aux responsables des systèmes d'information d'une part d'installer les produits nécessaires à l'utilisation de connexions chiffrées et d'autre part de mettre en œuvre les mesures permettant de bloquer les connexions non sécurisées, au moins depuis l'extérieur.

Ordinateurs portables

Les ordinateurs portables répondent à de réels besoins en matière de mobilité. Malheureusement cette mobilité en facilite grandement le vol ou la perte. Plus que le coût lié à la disparition d'une machine, le risque à considérer est celui de la divulgation de données confidentielles. Vouloir se contenter sur un ordinateur portable de traiter et stocker uniquement des données anodines ou publiques est illusoire. Les données les plus sensibles sont généralement celles sur lesquelles on travaille le plus activement. La seule façon de se prémunir est de chiffrer de façon robuste le contenu du disque afin que les informations qu'il contient ne puissent être exploitées par quiconque aurait récupéré la machine.
Parmi les différentes méthodes de chiffrement, il faut privilégier celles qui chiffrent la totalité du disque afin d'éviter que par inadvertance une information sensible ne se retrouve dans une zone non chiffrée.
Le chiffrement implique la mise en place de procédures de recouvrement efficaces permettant de récupérer les données en cas de perte ou d'oubli du secret protégeant la clé ce déchiffrement.
Pour les déplacements dans les pays qui interdisent le chiffrement ou présentent des risques particuliers en matière de confidentialité, ce sont souvent les mêmes, la prudence consiste à ne

pas emporter son ordinateur personnel mais un portable banalisé, réservé à cette usage, sur lequel on ne stockera que les informations strictement nécessaires.

Supports amovibles

Les supports amovibles (CD, DVD, clés USB) sont extrêmement commodes pour transporter des données. Du fait de leurs faibles dimensions, les risques de perte ou de vol sont encore bien plus élevés que pour les ordinateurs portables. Aussi, sauf pour les données par nature publique comme le contenu de la présentation que l'on va transférer sur l'ordinateur de la conférence, le chiffrement des supports amovibles s'impose.
Comme la plus élémentaire prudence veut que l'on conserve en lieu sûr une copie des données stockées sur un support amovible, la possibilité de recouvrement n'est pas critique.

Le numéro 62 du bulletin sécurité informatique[1] *traite avec plus de détails de la protection des données et du chiffrement.*

[1] http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num62.pdf

Annexe A : Typologie du chiffrement

Les besoins de confidentialité auxquels répond le chiffrement :

- Perte, vol de supports amovibles (CD, DVD, clé USB, bandes, etc.)
- Perte, vol ou emprunt temporaire (le temps de dupliquer le disque) d'ordinateur portables
- Vol de serveurs ou postes fixes
- Limitation à ceux qui ont à en connaitre de l'accès à des fichiers sur un poste de travail, un serveur, un partage en réseau (maintenance, téléassistance, partage de fichiers dans une collaboration de recherche, etc.)
- Mise au rebut ou réparation de disques
- Communications sur le réseau
- Echanges de messages (courrier électronique) et transferts de fichiers sur le réseau
- Protection contre l'espionnage de données particulièrement sensibles

Types d'utilisations :

- Nomadisme : portables, supports amovibles, connexions à distance
- Protection des données confidentielles, limitation aux seuls qui en ont à connaitre
- Gestion de parc : mise au rebut, réparation
- Protection contre le vol de serveurs, postes de travail fixes
- Echanges de documents confidentiels sur le réseau

Sensibilité des données

- Publiques ou ouvertes
- Diffusion limitée
- Sensibles (901)
- Classifiées (900) : hors champ.

De qui veut-on se protéger ?

- Opportunistes ou occasionnels
- Pirates, de malveillants, des écoutes passives, etc.
- Agences étrangères
- Intelligence économique ou autre.

Métadonnées

- Existence ou non
- Duplication ou non (redondance en cas de problème comme un secteur défectueux)
    - Interne

- Externe

Robustesse du chiffrement

- Algorithme utilisé (AES, DES, etc.)
- Mode de chiffrement et gestion des IV (CBC, LWR, etc.)
- Longueur de la clé (56, 128, 256)
- Implémentation, c'est généralement là que cela pèche
- Présence éventuelle de portes dérobées

Protection de la clé symétrique de chiffrement

- Dérivée du mot de passe par un hash
- Aléatoire et chiffrée par un hash du mot de passe
  - Ajout ou non d'un salt pour le calcul du hash
  - Itération ou non du hash pour allonger le temps de calcul
- Aléatoire et chiffrée par une clé publique (certificat)
- Niveau supplémentaire de chiffrement de la clé (permet de révoquer des autorisations sans rechiffrer tout le disque). Exemples : ZoneCentral, BitLocker
- Chiffrée plusieurs fois (certificat ou mot de passe) pour permettre le recouvrement

Niveau (granularité) du chiffrement

- Disque dur avec chiffrement intégré au matériel
- Disque ou partition
  - Clé fournie avant le « boot »
  - Clé fournie après le « boot »
- Système de fichiers chiffré
- Conteneur chiffré à la ZIP ou disque virtuel
- Ensemble des fichiers d'un répertoire
- Fichier
- Donnée dans un fichier ou un SGBD

Attention aux endroits où l'on pourrait trouver des données en clair

- Mémoire vive
- Fichiers temporaires
- Swap
- Dump en cas de crash du système
- Fichier d'hibernation (mise en veille)
- Informations dans les fichiers systèmes
  - Base de registre Windows
  - Secrets d'authentification (en particulier sous Windows)
  - Données de connexion : noms de serveur, identifiants, etc.
  - Fichiers de configuration. Exemple : mot de passe Filezilla (cf. Eurosec 2007)

- Cache et historique du navigateur
- Métadonnées (nom de fichiers)

Fenêtre d'exposition des données en clair

- Machine allumée
- Session utilisateur
- Du déverrouillage du répertoire ou fichier à sa fermeture

Méthode de recouvrement

- Séquestre : duplicata de la clé ou du mot passe en lieu sûr
- Agent de recouvrement : une autre personne a la possibilité de déchiffrer le fichier

Protection de la clé de chiffrement symétrique

- Mot de passe
- Certificat
    - Fichier
    - Dispositif matériel (carte à puce, token USB, TPM)

Coûts

- Intégrés aux systèmes d'exploitation
    - EFS (Windows)
    - FileVault (MacOS X)
    - Dm-crypt (Linux)
- Intégrés à une version spécifique du système d'exploitation
    - BitLocker : Windows Vista Ultimate ou Entreprise (Professionnel -> intégral = + 50€ chez Dell)
- Produits libres
    - TrueCrypt (Windows, Linux, MacOS X)
    - …
- Produits commerciaux
    - ZoneCentral : 70€
- Matériel
    - Disque chiffré. Exemple Seagate (120Go, 5400) sur portable Dell : + $130 (USA)
    - Clé USB chiffrée ou disque amovible avec processeur cryptographique intégré : quelques centaines d'euros

Limites du chiffrement

- Un keylogger peut récupérer un mot de passe. Un logiciel espion peut à l'insu de l'utilisateur légitime qui accède à ses données chiffrées retrouver en mémoire les clés de chiffrement ou tout simplement les données déchiffrées.

- Les imprimantes.
- Ingénierie sociale

Visibilité des zones chiffrées

- Clairement affichées comme étant chiffrées : signature
- Masquées ou dissimulé dans d'autres données : déni plausible

Annexe B : Inventaire de solutions

- EFS
  - Windows
  - Système de fichiers chiffré
  - Certificat
  - Inclus dans Windows
- ZoneCentral
  - Windows
  - Chiffrement de tous les fichiers d'un répertoire
  - Certificat ou mot de passe
  - 70€
- BitLocker
  - Windows Vista
  - Partition
  - TPM, clé USB, code PIN
  - 0 à 50€ (inclus dans entreprise et intégrale, +50€ professionnelle -> intégrale)
- FileVault
  - MacOS X
  - Système de fichiers chiffré
  - Certificat
  - Inclus dans MacOS X
- Ecryptfs
  - Linux
  - Système de fichiers chiffrés. Chaque fichier possède ses propres métadonnées dont la clé symétrique.
  - Certificat ou mot de passe ou TPM
  - Inclus dans la plupart des distributions Linux
- Dm-crypt/cryptsetup
  - Linux
  - Partition
  - Mot de passe
  - Inclus dans la plupart des distributions Linux
- TrueCrypt
  - Windows (NTFS, FAT), Linux (ext3, FAT), MacOS X
  - Chiffrement integral du disque sous Windows avec authentification au démarrage.
  - Disque virtuel dans un fichier, une partition ou un disque
  - Mot de passe
  - Open source
- SafeBoot
  - Windows
  - Disque. Authentification avant le boot

- Mot de passe, certificat, carte à puce

Annexe C : Recommandations techniques

Communications

- Utiliser les protocoles sécurisés : normalisés comme SSL/TLS, IPSec ou standards comme SSH, OpenVPN
- Ils sont de fait déjà largement utilisés

Courrier électronique, échanges de fichiers

- S/MIME pour les destinataires qui ont un certificat X509 voire PGP pour ceux qui ont une clé PGP
- Sinon utiliser un conteneur chiffré
    - Il reste à évaluer et conseiller des outils parmi les nombreux existants
    - Reste dépendant de ce qu'acceptent le destinataire et sa passerelle de messagerie (filtrage des pièces jointes).

Ordinateurs portables

- Seule une solution qui chiffre l'intégralité du disque permet de se prémunir contre toute fuite d'information. Cela est particulièrement vrai sous Windows où les fichiers systèmes et utilisateurs ne sont pas rangés sous des répertoires clairement séparés. Mais entre le souhaitable et le possible, il faut bien accepter des compromis.
- Disque chiffré
    - Indépendant de l'OS
    - Mot de passe au niveau du BIOS (du moins je présume)
    - Encore jeune, non testé
- Bitlocker
    - Windows Vista intégrale ou entreprise
    - Partition entière chiffrée y compris swap et hibernation
    - Mot de passe facultatif si TPM
- Autres versions de Windows
    - TrueCrypt
    - Pourquoi pas SafeBoot qui bénéfice d'un accord dans le cadre du groupe logiciel (vient d'être racheté par MacAfee).
    - EFS car standard et donc gratuit mais attention à tout ce qui en dehors des répertoires chiffrés (temporaires, swap, hibernation).
    - Dans le cas où ZoneCentral est déployé dans l'unité pour d'autres usages, il est possible de l'utiliser pour les portables avec une politique de chiffrer tout sauf le système. Le swap est chiffré mais pas le fichier d'hibernation (pas de mise en veille prolongée).
- Apple
    - FileVault ou TrueCrypt

- Linux
    - Chiffrement du swap avec dm-crypt (inclus dans la plupart des distributions)
    - Chiffrement d'une partition avec dm-crypt/cryptsetup dans laquelle on mettra /home, /tmp, /var
    - Les distributions récentes ou a venir dans un futur proche (Fedora 9 est annoncé fin avril 2008) permettent de chiffrer la partition racine et d'effectuer l'installation sur des partitions chiffrées. C'est la meilleure solution pour les portables.

Mise au rebut ou réparation

- Confortable mais ne justifie pas à lui seul le chiffrement, ne peut être qu'un sous produit d'une solution de chiffrement pour un autre usage.
- Détruire ou purger le disque avant mise au rebut. Il existe des logiciels gratuits et faciles à utiliser de purge de disque.
- Prévoir des contrats de maintenance qui précisent que l'on conserve le disque en panne.

Clés USB

- Conteneur chiffré (disque virtuel). TrueCrypt semble la solution de choix.

Protection contre le vol des serveurs

- Il est généralement préférable de sécuriser la salle contenant les serveurs

Protection contre le vol de postes fixes ou l'aspiration de données

- Sécurisation des locaux
- Idem ordinateurs portables ou protection des données confidentielles

Protection des données confidentielles, limitation aux seuls qui en ont à connaitre

- Chiffrement des fichiers/répertoires contenant les données sensibles. Déchiffrement par la personne autorisée au moment de l'utilisation.
- Sous Windows avec des partages en réseau : ZoneCentral. Sans partage réseau EFS peut suffire.
- MacOS : FileVault
- Linux : Ecryptfs voire dm-crypt

Annexe D : Recommandations en matière d'organisation

Suivre les évolutions

- Les systèmes d'exploitation, les matériels intègrent de plus en plus le chiffrement car c'est un besoin qui se fait de plus en plus sentir. Les évolutions sont très rapides aujourd'hui.
- Savoir abandonner en douceur un produit qui répondait à un besoin à un moment donné mais qui de fait de l'évolution du marché peut être satisfait de façon plus simple et à moindre coût.

Mettre en place les structures pour le recouvrement

- Privilégier la simplicité
- Une enveloppe contenant le mot de passe au secrétariat du laboratoire plus éventuellement une autre à son domicile est une solution acceptable pour le chiffrement des portables
- Pour les supports amovibles qui servent uniquement à transporter les informations d'une machine à une autre on peut se dispenser de séquestre ou recouvrement (la source existe toujours).
- Pour les solutions qui utilisent un agent de recouvrement, prévoir des méthodes de distribution ou déploiement du produit qui intègre automatiquement la clé publique de l'agent de recouvrement
- Les disques surtout ceux des portables ont un taux de défaillance relativement important (quelques % par an). Les sauvegardes sont indispensables. Il ne faut donc pas surévaluer le risque de perte de données parce que le recouvrement aura été impossible vis-à-vis de la panne du disque.

IGC du CNRS

- Ajouter dans les certificats les attributs nécessaires pour qu'ils soient acceptés par les différents produits de chiffrement comme EFS, peut-être FileVault (à vérifier)
- Créer de vrais certificats de chiffrement distincts de ceux servant à l'authentification.
- Le séquestre des certificats de chiffrement est une possibilité qui mériterait réflexion.

Traiter la confidentialité dans tous ses aspects

- Le chiffrement ne résout pas tous les problèmes de fuite d'information
- Poste de travail compromis
- Autres canaux : imprimante, capture d'écran
- Ingénierie sociale

Déploiement, assistance, documentation

- Préparer des versions préconfigurées pour le déploiement (charge de travail estimatif : 15 j par package, au moins 5 packages à prévoir)
- Mettre en place une structure d'assistance (une personne à ¼ ou ½ temps)
    - Hot line : ASR
    - Conseil : CRSSI
- Rédiger des documentations (1 mois par doc, une doc par package)
- La vraie question est qui va le faire ?
- Catalogue

Annexe E : Plan d'action

Chiffrer l'ensemble des portables

- Chiffrement intégrale du disque.
- Sur une période de 3 ans, durée de vie moyenne d'une machine (l'installation du chiffrement ne peut se faire raisonnablement que sur une machine neuve).
- N'installer désormais que des portables chiffrés.
- Revoir en ce sens les marchés.

Sécuriser les communications sur Internet

- Chiffrer les communications contenant des informations un tant soit peu sensibles, personnelles. Impérativement aucun mot de passe ne doit circuler en clair.
- Les protocoles, les produits existent et sont déjà largement employés.
- Echéance : le plus rapidement possible. Aujourd'hui un Telnet, un FTP ou une application Web qui expose le mot de passe en clair n'est pas acceptable.
- Rappeler la règle et diffuser les documentations sur la mise en œuvre des protocoles sécurisés (elles existent déjà).

Chiffrer les supports amovibles

- Lorsque c'est possible. Difficile de chiffrer la présentation sur la clé que l'on introduit dans l'ordinateur de la conférence.
- Utiliser un conteneur chiffré (disque virtuel). TrueCrypt est un bon candidat.
- En ce qui concerne le bureau intégré sur une clé (applications et données sur une clé USB U3), il faut conduire une étude de la sécurité pour déterminer si et dans quelles conditions on peut le recommander.
- Faire des recommandations, rédiger et diffuser de la documentation.
- Echéances : aboutir rapidement aux recommandations et à la documentation, ensuite y aller progressivement sachant qu'il n'est pas besoin d'attendre un remplacement du matériel.

Echanges de documents par courrier électronique

- Si le destinataire a un certificat X509 ou une clé publique PGP, pas de vrai problème la bonne version du client de messagerie avec éventuellement le bon plugin suffit.
- Sinon il faut échanger un conteneur chiffré et transmettre par un autre canal le mot de passe.

Chiffrer les documents confidentiels (poste de travail ou partage réseau)

- Le chiffrement doit être effectué sur le client et non le serveur.
- Chiffrement de répertoire : ZoneCentral ou éventuellement EFS s'il n'y a pas de partage (Windows), Ecryptfs (Linux).
- Bien valider les procédures de recouvrement car c'est là qu'elles sont critiques.

Opération pilote

- Adresser l'ensemble des problématiques du chiffrement, des systèmes d'exploitation et ne pas se limiter au déploiement d'un produit sur une seule plateforme. On testera donc plusieurs solutions.
- Objectifs : déterminer
    - Les ressources financières et humaines liées au déploiement du chiffrement.
    - Les besoins de formation et d'assistance des administrateurs et des utilisateurs.
    - L'acceptation par les utilisateurs.
    - La vérification en situation réelle des procédures de recouvrement.
- Dans un contexte où une solution unique ne peut répondre à tous les besoins il faut bien accepter une multiplicité de produits. Par contre au niveau organisationnel, il doit être possible de standardiser l'installation et le déploiement, l'assistance, les procédures de recouvrement ou de séquestre.