

• Éditorial par **R. Longeon**

• Le chiffrement au CNRS : analyse et recommandations par **F. Morris**

• Que protéger? Ou comment « cibler » les données « sensibles » par **J. Illand**

SÉCURITÉ INFORMATIQUE

numéro 62 Décembre 2007

SÉCURITÉ DES SYSTÈMES D'INFORMATION

éditorial

Pour les données aussi sortez couverts...

Il est des solutions qui engendrent des problèmes plus graves que ceux qu'elles résolvent... ou sont censées résoudre. C'est souvent le cas en SSI lorsqu'on oublie combien le lien entre « technique », « facteurs humains » et « organisation » est étroit. Un bon exemple nous est donné avec le chiffrement. Certes, les **facteurs techniques** doivent être étudiés soigneusement afin de ne pas utiliser des produits de chiffrement qui ne soient qu'une simple poudre de « Perlimpinpin ». Il en existe...

Toutefois, est-ce suffisant? Non! Personne ne contestera, par exemple, la nécessité de chiffrer les données des ordinateurs portables ou des clés USB tant le risque de perte ou de vol est grand, mais si vous avez un trou de mémoire inopiné et irrémédiable au moment de taper votre mot de passe, qu'est-ce que vous faites? Autre exemple, votre système s'est figé pendant l'opération de chiffrement de la partition contenant vos données confidentielles; vous avez dû alors redémarrer votre ordinateur à chaud et, depuis, vous ne voyez plus cette « maudite » partition. Que croyez-vous qu'il adviendra?

Moralité: sans une procédure de recouvrement, sans sauvegardes des données, le chiffrement n'est à conseiller qu'à ceux qui aiment vivre dangereusement; les personnes plus avisées savent, quant à elles, qu'il faut établir des règles (partie intégrante de la politique de sécurité) qui rendent ces opérations sûres (**facteurs organisationnels**).

Reste que chiffrer un fichier ne sert à rien si une personne malveillante peut le retrouver en « clair » ailleurs. Or les situations où il est ainsi recopié – à l'insu de l'utilisateur – ne manquent pas: fichiers temporaires enregistrés à discrétion par les logiciels sous Windows et rarement effacés proprement, fichiers de veille prolongée des ordinateurs portables, fichier « swap », fichiers d'impressions, etc. N'oublions pas non plus que les méthodes « d'ingénierie sociale », les « keyloggers », « l'écoute réseau » et les chevaux de Troie permettent, mieux que « la force brute », de récupérer les mots de passe.

Moralité: le niveau de confidentialité d'un fichier chiffré dépendra donc de l'attention que l'utilisateur portera aux contrôles de ce type de fichiers, temporaires ou non (**facteurs humains**).

Développer une solution de chiffrement, c'est prendre en compte ces trois facteurs tout en se gardant de générer des structures trop bureaucratiques qui, à l'échelle d'un organisme comme le nôtre, seraient forcément lourdes et coûteuses. L'approche que développe François Morris dans ce numéro est pragmatique; à la complexité du problème, il propose non pas LA solution bonne à tout faire, mais des réponses diverses, adaptées à chacun des besoins. Joseph Illand, quant à lui, nous rappelle nos obligations vis-à-vis des données sensibles. Protégez vos données, nous disent-ils, mais pas seulement avec de bonnes intentions... surtout avec celles dont on pave l'enfer.

Robert Longeon

Chargé de Mission à la sécurité des systèmes d'information au CNRS

Le chiffrement au CNRS : analyse et recommandations

Par **François Morris**

Ingénieur de recherche à l'Institut de minéralogie et de physique des milieux condensés (IMPMC), Expert SSI auprès du FSD

Protéger les informations confidentielles ou sensibles des oreilles et des regards indiscrets est un impératif. Cela peut être une obligation légale ou réglementaire, faire partie des clauses d'un contrat ou tout simplement résulter de la défense bien comprise de ses propres intérêts. Il est important de bien appréhender combien la non-protection de données confidentielles peut aboutir à de graves conséquences.

La responsabilité pénale peut être engagée. Ainsi, la loi « informatique et libertés » prévoit cinq ans d'emprisonnement et 300 000 € d'amende si toutes les précautions utiles pour préserver la sécurité des données à caractère personnel n'ont pas été prises.

Le non-respect de clauses de confidentialité dans un contrat engage sa responsabilité civile et peut entraîner le versement de dommages et intérêts considérables ou plus prosaïquement empêcher d'établir de nouveaux contrats et donc tarir une source importante de financement de la recherche.

Pourquoi et que chiffrer?

Si on prétend faire de la recherche de qualité, il y a nécessairement des informations de valeur à protéger et une réputation à maintenir. Que l'on pense aux dépôts de brevets ou tout simplement au fait d'être le premier à publier une découverte!

En empêchant qu'une information tombée entre des mains inamicales puisse être directement exploitée, le chiffrement est un moyen de réaliser cet objectif de protection des données. Cependant, ce n'est qu'un moyen parmi d'autres, il vient en complément d'autres mesures de nature organisationnelle comme la sécurité physique.

Chiffrer permet, quand les aspects organisationnels sont correctement pris en compte, de réduire notablement, faute de pouvoir l'éliminer totalement, le risque de divulgation d'informations confidentielles. Mais chiffrer a aussi un coût qui se suite page 2 >>>

traduit en termes de matériels, de logiciels et plus encore en contraintes organisationnelles. La décision de chiffrer devrait donc être essentiellement fondée sur une analyse de risques. Sans entrer dans les détails, une évaluation du risque fait entrer en ligne de compte les conséquences d'une fuite incontrôlée d'informations, la vraisemblance d'occurrence de la menace, la facilité d'exploitation. Il faut aussi mettre en balance l'introduction d'un nouveau risque induit, qui est celui de se retrouver dans l'impossibilité de déchiffrer les informations.

S'il n'est pas utile de chiffrer une information anodine, il peut s'avérer finalement plus simple et moins coûteux de ne pas distinguer la sensibilité des informations situées sur un même support et alors de tout chiffrer. Par ailleurs, le recoupement d'un ensemble d'informations dont chacune est *a priori* non sensible peut conduire à retrouver une information finalement sensible.

Les mesures préconisées dans cet article ne s'adressent pas aux informations classifiées de défense qui doivent être traitées selon des procédures spécifiques.

Comment chiffrer ?

La multiplicité des besoins, la diversité des situations, les limites des produits disponibles ne permettent pas de proposer une solution unique qui soit applicable partout. Si le choix du ou des produits utilisés ne peut, *in fine*, que relever d'une décision au niveau local, celui de l'unité, on ne peut pas laisser l'utilisateur final livré à lui-même sans aucune

aide. Il convient aussi de ne pas multiplier à l'infini les solutions afin de profiter d'une mutualisation des efforts. C'est pourquoi il a été établi un certain nombre de préconisations pouvant s'appliquer aux différents cas. Les critères de facilité et de coût en matière de déploiement et d'utilisation ont été privilégiés, en considérant que, dans certains cas, une solution même incomplète est préférable à une absence totale de chiffrement. Cela signifie qu'implicitement on cherche d'abord à se protéger des menaces provenant d'opportunistes, plutôt que de celles d'attaquants déterminés possédant des moyens importants et menant une attaque ciblée (ces derniers ont sans doute bien d'autres moyens que la cryptanalyse pour parvenir à leur fin, ne serait-ce que l'ingénierie sociale).

Ordinateurs portables

Le nombre d'ordinateurs portables croît fortement, les utilisateurs y stockent désormais l'ensemble des informations sur lesquelles ils travaillent. Il n'est pas exagéré de dire que nombre d'informations des plus sensibles se trouvent désormais sur des ordinateurs portables. La perte d'une machine ou son oubli dans un lieu public est un événement fréquent (plus d'une centaine par an pour le CNRS). Le vol en est relativement aisé. Il ne faut pas non plus négliger l'emprunt temporaire, le temps de recopier le contenu du disque est d'autant plus dangereux qu'il a toutes les chances de passer inaperçu. Si, évidemment, il faut commen-

cer par faire attention et surveiller sa machine, seul le chiffrement permet de protéger efficacement la confidentialité des informations.

Chiffrer uniquement une partie du disque (répertoire, disque virtuel) dans laquelle vont être enregistrés les fichiers sensibles de l'utilisateur exige de pouvoir contrôler strictement l'emplacement où l'utilisateur va écrire ses fichiers. Cela implique la mise en œuvre des fonctionnalités de contrôle d'accès du système d'exploitation, l'expérience a montré qu'indépendamment de tout chiffrement le simple fait de positionner des droits sur des fichiers est très difficile à mettre en pratique. Il faut aussi prendre garde à tous les emplacements où pourraient subsister des données en clair : fichiers temporaires, fichier d'échange (swap), fichier d'hibernation pour la mise en veille prolongée, base de registres sous Windows. C'est pourquoi la solution la plus simple consiste à chiffrer l'intégralité du disque, l'authentification se faisant alors avant le démarrage du système.

Des disques intégrant un dispositif matériel de chiffrement commencent à apparaître sur le marché. C'est sûrement une excellente solution, indépendante du système d'exploitation qu'il faut envisager lors de l'acquisition d'un ordinateur portable. Les versions «intégrale» et «entreprise» de Windows Vista intègrent BitLocker, un outil de chiffrement de disque. Sur les machines qui intègrent un dispositif cryptographique matériel (la puce TPM, Trusted Module Platform), ce qui devient de plus en plus courant, la sécurité offerte par BitLocker est renforcée et il est possible de [suite page 3](#)

Chiffrement sous Linux

Les versions récentes du noyau Linux intègre «dm-crypt», un dispositif transparent de chiffrement à la volée qui permet de chiffrer des disques entiers, des partitions, des volumes logiques ou des fichiers. LUKS (Linux Unified Key Setup), un standard pour les métadonnées associées au chiffrement, facilite grandement la gestion des volumes chiffrés.

Le système est suffisamment souple pour s'adapter aux différentes situations :

- pour un exemple de chiffrement sur un portable : <http://www.impmc.jussieu.fr/~morris/chiffrement/luks.html>
- pour un système multiutilisateur, on trouvera une élégante méthode pour permettre à chacun de choisir son propre mot de passe tout en ayant une clé générale pour le recouvrement : http://www.hsc.fr/ressources/brevets/cryptsetup_luks.html

Chiffrement sous Windows avec EFS

EFS (Encrypted File System), qui existe depuis Windows 2000, ne fonctionne qu'avec le système de fichiers NTFS.

Recouvrement dans EFS : la clé de chiffrement symétrique est elle-même chiffrée par la clé publique du propriétaire et celle d'un ou de plusieurs agents de recouvrement. Pour déchiffrer un fichier, il faut connaître au moins une des clés privées. Pratiquement, le propriétaire possède son certificat et l'agent de recouvrement le sien.

Un rapide essai a montré que la fonction recouvrement est correctement prise

en compte par EFS. La difficulté de son utilisation au CNRS vient du fait qu'il manque aux certificats délivrés par notre IGC des valeurs propriétaires Microsoft dans l'attribut «Utilisation avancée de la clé», il faudrait donc modifier notre IGC pour permettre l'utilisation de ce logiciel dans de bonnes conditions, ce qui devrait se faire sans grande difficulté avec openssl. De toute façon, les bonnes pratiques recommandent que les certificats de chiffrement soient distincts de ceux qui servent à authentifier une personne. (Voir l'ensemble de l'article sur <http://www.impmc.jussieu.fr/~morris/chiffrement/EFS.html>)

- Le document technique de Microsoft sur EFS <http://www.microsoft.com/technet/security/topics/cryptographyetc/efs...>
- Quelques articles sur les bonnes pratiques pour chiffrer avec EFS <http://support.microsoft.com/kb/223316/en-us>
<http://support.microsoft.com/kb/241201>
<http://support.microsoft.com/?id=308989>
<http://support.microsoft.com/?id=308993>
<http://support.microsoft.com/?id=307877>
<http://support.microsoft.com/?id=308991>

Quelques conseils pratiques pour le chiffrement d'un disque dur

<http://www.impmc.jussieu.fr/~morris/chiffrement/Disques.html>

se dispenser d'avoir à fournir un mot de passe au démarrage; ce qui rend le chiffrement totalement transparent. Pour les autres versions de Windows, le produit de SafeBoot (nouvellement acquis par McAfee) permet de chiffrer l'intégralité du disque, y compris fichier d'échange et hibernation, avec une authentification avant le démarrage du système; un accord a été passé avec le groupe logiciel. Le produit ZoneCentral de Prim'X1 (1), qui fait aussi l'objet d'un accord avec le groupe logiciel, ne chiffre pas l'ensemble du disque dur, mais il est possible de le configurer pour chiffrer tous les répertoires où l'utilisateur pourrait enregistrer des fichiers, ainsi que le fichier d'échange, mais à l'exclusion du fichier d'hibernation. Dans le cas où ce produit est déployé par ailleurs pour protéger des partages de fichiers cette solution peut être envisagée afin de ne pas multiplier les solutions de chiffrement. Le système de fichiers chiffrés EFS se restreint au chiffrement de répertoires mais est disponible en standard sur toutes les versions de Windows (et donc gratuit, contrairement aux produits précédents). Il vaut mieux l'utiliser en connaissant ses limites, plutôt que de ne rien chiffrer faute d'avoir pu se procurer un produit plus adapté.

Si la plupart des distributions Linux intègrent un outil (dmccrypt/cryptsetup) qui permet de chiffrer des partitions, y compris le swap, actuellement rien n'est prévu en standard pour démarrer sur une partition racine chiffrée. Ce n'est cependant pas si grave que cela car, si les répertoires /home, /var, /tmp sont chiffrés, il n'y a quasiment aucun endroit où l'on puisse trouver des fichiers utilisateur en clair. Pour les Macintosh, à notre connaissance, le seul produit de chiffrement disponible est FileVault qui fait partie de Mac OS X. Le moment idéal pour déployer le chiffrement est lors de la mise en service d'une nouvelle machine, car chiffrer un disque qui contient déjà des informations est une opération délicate qui ne peut s'envisager qu'après une bonne sauvegarde de l'ensemble des données de l'utilisateur.

Certains pays présentent des risques particuliers en matière de confidentialité, d'autres interdisent le chiffrement, ce sont d'ailleurs souvent les mêmes. La bonne démarche, guidée par la prudence, consiste à ne pas emporter son ordinateur personnel mais un portable banalisé, réservé à cet usage, sur lequel on ne stockera que les informations strictement nécessaires. Au retour, on procédera à l'effacement du disque et à la réinstallation du système pour se prémunir contre les logiciels malveillants qui auraient pu y être ins-

tallés à son insu (les outils permettant de créer et de dupliquer des images de disques sont très utiles à cet effet).

Supports amovibles

Des supports amovibles, CD, DCD, disques, bandes et surtout clés USB servent à transférer les informations entre machines. La principale menace réside dans la fuite d'informations suite à la perte ou au vol du support. Le chiffrement est donc nécessaire, ce qui ne dispense pas bien évidemment de prendre des précautions et de ne pas laisser trainer les supports. Dans ce cas, la possibilité de recouvrement n'est pas critique puisqu'en principe les données originales sont toujours présentes (une personne sensée n'effacera pas l'original avant d'être sûr que le transfert s'est bien effectué).

La solution la plus adaptée consiste à utiliser un conteneur (disque virtuel) chiffré sur le support amovible. Il est souvent possible, au moins sous Windows, d'y inclure le logiciel permettant de déchiffrer les données, ce qui permet de relire les informations sur une autre machine sans rien avoir à installer. Ceux qui sont libres et gratuits sont à privilégier. Parmi les nombreux produits répondant à ce besoin, on peut citer TrueCrypt (2).

Communications

Il faut protéger des écoutes les données sensibles échangées sur un réseau en les chiffrant. Les outils servant au chiffrement des communications sont aujourd'hui bien maîtrisés et de fait largement utilisés. Parmi ceux-ci, on peut citer le protocole SSL/TLS qui sert à protéger les échanges entre clients et serveurs, SSH pour les connexions à distance sur une machine, IPSec ou openVPN (3) plus simple à mettre en œuvre pour établir des réseaux privés virtuels permettant d'interconnecter de façon sécurisée des machines ou des réseaux distants. Il faut noter que la plupart de ces protocoles impliquent l'utilisation de certificats, au moins du côté serveur, et la présence d'une IGC au CNRS facilite bien les choses. Parmi ces données sensibles, il y a les mots de passe utilisés pour l'authentification sur une machine, un service ou une application. Pratiquement, la protection de la phase d'authentification impose de protéger l'ensemble des échanges même si le reste des informations est relativement anodin. L'utilisation de protocoles non sécurisés comme telnet, FTP, POP3, IMAP ou bien http,

au lieu de https (application web) qui authentifie un utilisateur par mot de passe transisant en clair, doit être rigoureusement proscrite.

Courrier électronique

Le service du courrier électronique n'offre aucune confidentialité, c'est l'équivalent de la carte postale. Pour un destinataire qui possède un certificat électronique, l'utilisation de S/MIME pour chiffrer le contenu du message est la solution la plus pratique d'autant plus que ce protocole est supporté par la plupart des clients de messagerie et que son utilisation en est relativement simple, il suffit de cocher une case pour demander le chiffrement. Pour les autres situations, l'envoi en pièce jointe d'une archive chiffrée et la transmission du mot de passe par un autre canal comme le téléphone sont acceptables, du moins tant que l'on n'échange pas des informations particulièrement sensibles. Il existe différents produits permettant de chiffrer des archives, l'utilisation en est relativement simple car ils possèdent une interface proche de celle de ZIP.

Partage de fichiers

Le chiffrement est un moyen efficace pour limiter l'accès à des informations à ceux qui ont à en connaître. Le cas le plus évident étant d'éviter que l'administrateur du système puisse par exemple lire des informations confidentielles, tout en lui permettant d'effectuer les opérations de maintenance. L'autre situation concerne des fichiers partagés sur le réseau que seules les personnes habilitées doivent pouvoir lire. Dans le premier cas, un outil de chiffrement de répertoire ou de disque virtuel chiffré répond au besoin. On peut citer à nouveau les « produits libres » ou intégrés au système, comme EFS pour Windows, dmccrypt pour Linux, FileVault pour Mac OS X, voire TrueCrypt pour Windows ou Linux. Dans le deuxième cas, les fichiers doivent être chiffrés/déchiffrés à la volée sur le poste de travail lors de leur écriture/lecture. Les produits qui répondent à cette exigence sont peu nombreux. Sous Windows, nous recommandons ZoneCentral de Prim'X. Sous Linux, on trouve le système de fichiers chiffrés eCryptfs (4).

1. <http://www.primx.eu/>

2. <http://www.truecrypt.org/>

3. <http://openvpn.net/>

4. <http://ecryptfs.sourceforge.net/>

Données externalisées

Souvent, pour d'excellentes raisons, on est amené à stocker des données à l'extérieur. C'est le cas des sauvegardes, la plus élémentaire prudence exige que l'on conserve une copie à l'extérieur du site afin de faire face à un sinistre comme un incendie ou une inondation. Cela peut être, pour les mêmes raisons que précédemment, la réplication d'une baie de disques sur un autre site. Il est impératif de chiffrer des données externalisées et cela devrait être prévu dès la conception du projet.

Organisation

Les obstacles au déploiement du chiffrement résident moins dans la technique ou même le coût (il existe des produits intégrés aux systèmes d'exploitation ainsi que des produits libres qui sont à maints égards satisfaisants) que dans les aspects humains et organisationnels.

Paradoxalement l'existence d'un mécanisme de recouvrement a fait apparaître une nouvelle inquiétude, celle que celui qui possède la clé de recouvrement puisse accéder aux données à l'insu de leur propriétaire. À cela on peut répondre que l'organisation mise en place et la déontologie l'exclut et que, de toute façon, avant la mise en œuvre du chiffrement l'accès était encore plus simple !

Les méthodes de recouvrement dépendent bien évidemment des possibilités des produits mais certains proposent le choix entre mot de passe, ce qui suppose un séquestre, et un certificat. L'utilisation de certificats n'implique pas nécessairement la présence d'un agent de recouvrement, il est toujours possible de sauvegarder le certificat de l'utilisateur, sa clé privée dans un fichier protégé par un mot de passe et de ranger l'ensemble dans un coffre. La décision d'employer une méthode plutôt qu'une autre doit dépendre du contexte local, mais il faut rester pragmatique et privilégier la simplicité, sans oublier qu'un certificat stocké avec sa clé privée dans un fichier protégé par un mot de passe n'offre guère plus de sécurité qu'un simple mot de passe. D'un autre côté, un déploiement à grande échelle sera certainement plus simple, s'il est possible de diffuser massivement un produit préconfiguré avec le certificat de recouvrement.

La mise en œuvre d'une solution de chiffrement impose généralement la fourniture par l'utilisateur d'un mot de passe supplémen-

Recouvrement

Outre l'obligation légale de fournir, sur réquisition des autorités judiciaires, «les conventions de déchiffrement», il faut se garantir contre une menace nouvelle, dont les conséquences peuvent être catastrophiques, celle de ne plus pouvoir accéder aux données en cas de perte du secret qui a servi au chiffrement... ou de défaillance volontaire ou involontaire de son détenteur. Pour cela, il est impératif de mettre en place une forme d'organisation qu'on appelle ordinairement «procédures de recouvrement». La première de ces formes consiste à confier à un tiers, l'agent de recouvrement, la possibilité de déchiffrer les informations indépendamment de leur propriétaire. La seconde consiste à sauvegarder en lieu sûr les secrets de chiffrement, on parle alors de séquestre. Ces deux types de procédures sont déjà couramment pratiquées. L'administrateur qui, sur un système, a la possibilité de relire les données d'un utilisateur ou de changer son mot de passe n'est jamais, en ce sens, qu'un agent de recouvrement. On devrait toujours conserver en lieu sûr un séquestre du mot de passe de l'administrateur d'une machine, d'un matériel réseau, d'une application ou d'un SGBD. Il est vrai que l'on s'en dispense parfois, sachant qu'il existe une méthode de réinitialisation de ce mot de passe à la suite d'un redémarrage particulier (à partir d'un CD, en appuyant sur un bouton à la mise sous tension par exemple). Attention, le fait de chiffrer un disque peut interdire de réinitialiser le mot de passe en redémarrant le système à partir d'un CD.

Techniquement, et sans entrer dans les détails, il existe deux méthodes pour protéger le secret utilisé lors des opérations de chiffrement/déchiffrement des données. La première consiste à chiffrer ce secret à l'aide d'un mot de passe ; le recouvrement se fera alors par séquestre de ce mot de passe. La seconde consiste à utiliser la cryptographie asymétrique en chiffrant le secret deux fois : la première fois avec la clé publique du propriétaire des données, la deuxième fois avec celle de l'agent de recouvrement (ce dernier n'a pas à être présent puisque l'on utilise une clé qui est publique par définition). Pour accéder aux données, le propriétaire fournira sa clé privée, elle-même protégée par un mot de passe, l'agent de recouvrement pourra aussi y accéder en fournissant sa propre clé privée.

L'organisation du séquestre est relativement simple. Généralement il suffit d'inscrire le mot de passe sur une feuille de papier ou/et le stocker dans un fichier sur une clé USB ou un CD et de ranger le tout dans un lieu sûr, sous enveloppe cachetée, ce qui permet de savoir que le séquestre a été utilisé. Un coffre-fort n'est pas forcément nécessaire, dans bien des cas une simple armoire fermée à clé dans un secrétariat fera l'affaire.

Pratiquement, le fait qu'une solution de chiffrement utilise un agent de recouvrement se traduit par la mise en place d'un certificat de recouvrement. Afin de faciliter la gestion, il est important de ne pas multiplier les certificats et d'utiliser le même pour tous les produits utilisés. L'IGC du CNRS délivre des certificats permettant le chiffrement.

La possibilité de recouvrement n'est pas nécessaire lorsque l'on possède l'original en clair des données chiffrées. On n'insistera jamais assez sur l'importance de procédures de sauvegardes efficaces et robustes. Le risque de perdre des données à la suite d'une panne de disque ou d'une erreur de manipulation est loin d'être négligeable et probablement supérieur à celui de perte d'un mot de passe.

taire. C'est contraignant et généralement contre-productif en matière de sécurité (la difficulté à mémoriser plusieurs mots de passe peut conduire à choisir le même partout ou à les écrire sur une étiquette). Si l'utilisation du même mot de passe pour chiffrer son disque et se connecter à sa messagerie est une aberration en matière de sécurité, mettre en place une authentification à deux facteurs avec un mot de passe et un élément matériel (carte à puce, clé ou token USB) offre un niveau de sécurité accru qui permet raisonnablement de répondre de façon unique à tous les besoins que ce soit le chiffrement ou la connexion à une machine.

Perspectives

Le déploiement du chiffrement ne peut se faire en un jour, il convient donc de s'attacher prioritairement aux données les plus sensibles et aux stockages les plus vulnérables. L'objectif serait de parvenir sur une période

d'environ trois ou quatre ans (la durée de vie des machines) à chiffrer l'ensemble des ordinateurs portables, du moins ceux qui contiennent des informations sensibles en mettant en place le chiffrement lors de l'installation de nouvelles machines. Pour les supports amovibles, on peut espérer un délai nettement plus court de l'ordre d'une année, le temps de mettre en place les procédures.

En ce qui concerne le chiffrement des communications, cela devrait déjà être systématique chaque fois qu'une donnée un tant soit peu sensible (un mot de passe l'est assurément) transite sur le réseau. Les recommandations en la matière ont été diffusées à maintes reprises depuis plusieurs années. Il reste à convaincre les réfractaires. Des recommandations sur le choix des produits de chiffrement, des conseils et de la documentation sur leur mise en œuvre, des outils facilitant le déploiement (exemples, fichiers de configuration, etc.) seront disponibles sur le site web du CNRS. ■

Francois.Morris@impmc.jussieu.fr

Que protéger ?

Ou comment « cibler » les données « sensibles » ?

Chiffrer pour protéger: oui sur le principe, encore faut-il s'entendre sur ce que l'on doit « protéger ». Pour la commodité du vocabulaire, mais aussi parce que la terminologie est consacrée par les textes (voir encadré), on parlera de la protection d'informations ou de données « sensibles ».

Par Joseph Illand, Fonctionnaire de sécurité défense au CNRS

Définitions

Les informations sensibles recouvrent deux grandes catégories :

- **les informations « classifiées de défense »** sont des informations dont la divulgation serait de nature à nuire à la défense nationale, elles sont répertoriées en trois niveaux, par degré décroissant d'impératif de protection :

- niveau « très secret défense » ;
- niveau « secret défense » ;
- niveau « confidentiel défense ».

Ces informations sont peu courantes au CNRS. Elles concernent des unités travaillant sur des thèmes très sensibles en liaison avec des organismes ou sociétés relevant du secteur de la défense ou encore des responsables (direction générale par exemple) ou des experts amenés par leurs fonctions à connaître de telles informations. *On rappellera que seules peuvent prendre connaissance de documents classifiés les personnes ayant fait l'objet d'une décision d'habilitation au niveau au moins correspondant et ayant de par leur fonction le besoin d'en connaître.*

- **les informations « sensibles non classifiées de défense » ou dites plus simplement informations « sensibles » (par opposition à « classifiées »)** sont des informations dont la confidentialité, mais aussi la disponibilité et l'intégrité doivent être protégées, sans justifier pour autant une « classification de défense ».

Ce sont des informations dont la compromission, l'altération, le détournement ou la destruction seraient de nature à porter atteinte aux intérêts fondamentaux de l'État (défense nationale, patrimoine scientifique et technique), à des intérêts économiques ou industriels, ou même à des personnes (risques liés à des fonctions ou des déplacements de personnels ou encore atteintes à la vie privée).

Ces informations peuvent être de nature scientifique ou technique mais aussi administrative.

La protection de ces données peut parfois relever d'une obligation légale (cas, par exemple, des « données à caractère personnel » ou « données médicales »).

Dans de nombreux cas, les documents contenant des données sensibles sont identifiés par des marquages tels que « diffusion restreinte », « confidentiel, industriel », « confidentiel, personnel », « confidentiel, médical »

Ce type de données se rencontre beaucoup plus fréquemment au CNRS. Le travail engagé par le CNRS sur le chiffrement des données exclut d'ailleurs le champ des données classifiées et ne porte clairement, à ce stade, que sur les données « sensibles ».

Mais la difficulté est souvent pour l'émetteur et le récepteur de l'information, de prendre conscience du caractère sensible de cette information et d'avoir le réflexe de la protéger (c'est en particulier le cas lors d'échanges internationaux, de recherches

débouchant sur la prise de brevets, de travaux intéressant la défense ou des technologies sensibles ou proliférantes, de données à caractère personnel...).

Essai de typologie des données sensibles

Pour mieux cerner le besoin de protection de l'information qu'on manipule, on peut tenter de se référer à une typologie des « informations sensibles » définie selon la nature de l'information.

C'est ainsi qu'on attachera d'emblée une importance particulière à des données telles que :

- des données à caractère personnel (état de primes, dossiers de carrière, dossiers médicaux, documents liés à des sanctions ou à un contentieux...);
- des données comptables et financières;
- des données à caractère politique ou stratégique (données préparatoires à des décisions, analyses ou audits non destinés à être communiqués);
- des données relatives à des compétences ou à des savoir-faire (lorsque la divulgation de ces informations est susceptible de nuire aux intéressés ou à l'institution);
- données relatives à la valorisation des résultats de la recherche (en particulier lorsque ces informations se situent en amont d'une publication ou d'un dépôt de brevet);
- données relatives à des coopérations nationales ou internationales;
- données scientifiques ou techniques touchant à des intérêts de défense (recherches à caractère militaire ou dual, quand elles ne sont pas classifiées); recherches dont la compromission pourrait aider la prolifération des armes ou le terrorisme);
- données à caractère industriel (relevant de contrats industriels par exemple);
- données propres à la sécurité elle-même (plans de bâtiment, don- *suite page 6* ➔)

Les principaux textes

- Instruction générale interministérielle n°1300 /SGDN/PSE/SSD du 25 août 2003 sur la protection du secret de la défense nationale (http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/IG1300.pdf)
- Recommandation 901/DISSI/SCSSI du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense (<http://www.ssi.gouv.fr/fr/reglementation/901/index.html>)
- Guide ministériel n°730/SCSSI du 13 janvier 1997 sur les systèmes d'information et applications sensibles (<http://www.ssi.gouv.fr/fr/documentation/730.pdf>)
- Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée
- Code pénal, en particulier articles 410.1, articles 413.9 à 413.12, articles 226.13 à 226.27 et 432.9.

Quelques recommandations relatives aux données sensibles

Les documents sensibles doivent être transmis sous pli confidentiel et remis aux seuls destinataires ayant à en connaître. Ces documents doivent être conservés sous forme protégée (meubles fermés à clé).

La transmission en clair par messagerie doit être proscrite. L'utilisation de logiciels de chiffrement et en particulier l'utilisation de certificats électroniques avec l'outil de chiffrement activé est recommandée pour la transmission de tels messages.

La mise en ligne sur Internet de documents sensibles est à proscrire formellement. L'utilisation de certains matériels ou logiciels peut être incompatible avec le caractère sensible des informations traitées ou véhiculées; ces matériels ou logiciels font alors l'objet de notes d'alerte ou de recommandations spécifiques.

nées de surveillance, consignes spécifiques de « diffusion restreinte », états de laboratoires ou installations repérés eux-mêmes comme sensibles, plans d'intervention ou de crise, dossiers ou procédures d'habilitation).

La protection peut recouvrir différentes formes selon le type d'information : discrétion en matière de communication orale, chiffrement de fichiers informatiques, non-transmission par messagerie (ou alors avec chiffrement), marquage des documents, conservation sécurisée des documents.

Cette typologie est utile mais ne suffit pas. D'une part, car des données relevant de cette typologie ne sont pas forcément sensibles et, d'autre part, il serait illusoire et dangereux d'imaginer que toute donnée ne relevant pas d'une des catégories précitées est automatiquement du domaine public et n'a pas à être protégée.

Au-delà des textes réglementaires, des directives et des conseils, il y a lieu d'insister sur le nécessaire **bon sens** qui doit guider l'identification des données qu'on ne souhaite pas voir divulguer et la juste adaptation des mesures de précaution au degré de sensibilité de ces données.

Les émetteurs, destinataires, détenteurs ou porteurs d'informations « sensibles » sont bien souvent les mieux placés pour apprécier la « valeur » de l'information et le prix qu'ils attachent à sa protection... **pour autant qu'ils soient conscients** de cette valeur et des conséquences de la compromission, de l'altération ou de la perte de l'information.

Le contexte

Par ailleurs, la protection à définir doit tenir compte du contexte et du support de l'information. L'information est-elle écrite, orale, sous fichier informatique et, dans ce cas, est-ce une donnée stockée, archivée, en cours de traitement, sur un poste fixe,

sur un portable, sur un support mobile de stockage, est-elle transportée (par mail) etc. ?

Un responsable des ressources humaines évoquera un problème de personne différemment selon qu'il est à la cafétéria ou dans son bureau capitonné. Un document relatif à un projet de contrat industriel hautement confidentiel fera l'objet de soins plus attentifs lors d'un voyage en train, plutôt que dans un bureau fermé.

Là encore, le bon sens doit s'imposer.

Le besoin d'en connaître

Au-delà de la nature de l'information et de son contexte, on n'oubliera pas un troisième critère (essentiel), qui est le « *besoin d'en connaître* ». Une information sensible peut être connue et peut être échangée dans le cercle restreint de ceux qui ont le besoin et la légitimité de la connaissance de cette information, et ce dans un contexte et un instant donné.

Mme Dupont, gestionnaire RH des ITA de l'unité X, n'a pas à connaître les dossiers des chercheurs et, le lendemain de sa mutation, elle n'a plus aucune légitimité à prendre connaissance des données qu'elle traitait précédemment (sauf bien sûr dans une phase de recouvrement possible avec la personne qui lui succède). Ce besoin d'en connaître trouvera pour elle sa traduction informatique par le concept de « profil utilisateur ».

Les moyens de protection

Ces moyens varient en fonction de la nature, du contexte et des personnes impliquées. Les moyens doivent être efficaces, non contournables et adaptés au besoin.

On évitera la protection « incantatoire » que l'on trouve hélas bien souvent dans des mails sensibles, sans autre protection que le mot « confidentiel » en début ou en

fin de texte, avec une mention du genre « Attention, ceci est un mail confidentiel, si vous n'êtes pas concerné merci de ne pas le lire... ».

On évitera aussi de se faire piéger par l'ingénierie sociale, et si l'on reçoit un mail chiffré on ne laissera pas une impression papier du mail sur l'imprimante du couloir...

Il n'est pas non plus forcément utile de chiffrer un fichier confidentiel, même s'il traite d'informations sensibles, si le poste de travail est fixe, non relié à Internet et dans une pièce fermant à clé. On se posera quand même la question du mode de ménage des locaux...

Risques pénaux

Les informations classifiées sont protégées par le code pénal (articles 431.10 et 431.11) et les atteintes sont durement sanctionnées (jusqu'à sept ans de prison et 100000 € d'amende). Certaines informations « sensibles » sont également protégées par le code pénal, c'est le cas notamment des données informatiques « à caractère personnel » (articles 226.16 à 226.24). En l'occurrence, sont notamment sanctionnés : le défaut de déclaration à la CNIL de fichiers à caractère personnel (article 226.16) et l'insuffisance de protection des fichiers (article 226.17). ■

joseph.illand@cnrs-dir.fr

À Paris, au cours des six derniers mois :

20196 téléphones portables ;
918 assistants personnels ;
459 ordinateurs portables
ont été oubliés dans les taxis !

SÉCURITÉ INFORMATIQUE

numéro 62 décembre 2007
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :

JOSEPH ILLAND
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris-XVI
Tél. : 01 44 96 41 88
Courriel : Joseph.Illand@cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

Rédacteur en chef : ROBERT LONGEON
Chargé de mission SSI du CNRS
Courriel : robert.longeon@cnrs-dir.fr

ISSN 1257-8819
Commission paritaire n° 1010 B 07548
La reproduction totale ou partielle
des articles est autorisée sous réserve
de mention d'origine.