GUIDE SSI

Mettre en œuvre des moyens appropriés à la confidentialité des données

mai 2005

Fiche 3

MEDEF

Accompagner

Pour rappel, 80% des dommages au patrimoine informatique ou informationnel de l'entreprise proviennent de malveillances internes, volontaires ou non. Certaines de vos données électroniques sont sensibles et font partie du patrimoine immatériel de l'entreprise. Elles doivent donc être protégées.

Contrôler l'accès aux données et applications

■ **Identification et Profil** : Une organisation des profils utilisateurs et des moyens d'identification de chacun d'entre eux est le minimum obligatoire pour éviter l'accès libre à vos informations (voir risque légal fiche 2).

■ **Droits d'accès** : À chaque profil doivent être associés des droits d'accès liés aux prérogatives du salarié. Certaines informations doivent pouvoir être accessibles en lecture seule, d'autres en mise à jour ou suppression selon les responsabilités de chacun.

■ **Mots de Passe** : Les mots de passe sont préférentiellement codés sur 8 caractères alphanumériques changés régulièrement. Voir fiche 4.

■ **Administration** : Pour contrôler l'accès à votre réseau d'entreprise ou à chaque poste de travail, vous aurez recours à un minimum d'administration qui vous permettra, par exemple, de gérer aussi soigneusement les départs de personnels que les entrées (les codes d'accès d'un salarié qui quitte l'entreprise doivent être immédiatement bloqués).

Sécuriser les échanges

■ **Risques**. Si vous n'utilisez pas de solutions sécurisées, un tiers malveillant peut utiliser vos données sensibles à des fins frauduleuses et à vos dépens (usurpation d'identité ou de coordonnées bancaires, espionnage industriel…).

■ **Echanges sur Internet**. Dans le cadre d'une utilisation « standard » des moyens d'échanges électroniques de données sensibles (votre n° de carte bleue par exemple) la politique minimale des sites consiste à passer du mode standard sur Internet au mode sécurisé. Ce changement est visible par la mention « https» dans votre barre de navigation, accompagnée éventuellement d'un cadenas en bas à droite de votre navigateur. Le protocole https permet de chiffrer l'échange électronique pendant son transfert entre l'expéditeur et le destinataire, empêchant ainsi quiconque de le lire.

■ Echanges de données critiques et confidentielles (fiscales, juridiques, médicales, etc.…) ou liées au secret professionnel. La loi sanctionne la violation du secret professionnel dans le cas où les solutions adéquates n'auraient pas été utilisées :

➔ La première solution consiste à utiliser des outils de chiffrement intégrés à votre messagerie électronique, couplés avec des certificats. Ces solutions sont peu onéreuses, mais leur mise en œuvre n'est pas aisée et ne vous donne pas de garantie absolue.

➔ La deuxième solution consiste à utiliser des services de messagerie sécurisée, commercialisés par des sociétés spécialisées. Il est bien entendu conseillé de privilégier les services d'une société reconnue et pérenne, afin d'avoir le maximum de garantie. Ces offres reposent sur le principe suivant :

- connexion de l'émetteur du message à un site sécurisé et dépôt du message,
- notification (via un e-mail) par le serveur sécurisé au destinataire qu'il a reçu un message,
- téléchargement par le destinataire du message sur le serveur intermédiaire sécurisé. Toutes ces opérations et échanges se déroulent sous protocole d'échanges chiffrés https.

➔ La troisième solution consiste à utiliser des services de messagerie sécurisée, associés à des certificats de signature électronique. Cette solution permet non seulement une excellente sécurité au plan technique, mais assure également le caractère probant de l'échange grâce à la signature électronique.

Moyens existants

■ **La « signature électronique »**. Le mot « signature » est utilisé ici dans un sens élargi, mais il faut rappeler qu'en droit français, signature vaut identification.

■ **Composantes**. La signature électronique est formée de trois composantes

- le document porteur de la signature,
- la signature elle-même,
- le certificat électronique authentifiant le signataire.

■ **Technologie**. La signature électronique s'appuie sur une technologie appelée PKI (Public Key Infrastructure, ICP : Infrastructure à Clefs Publiques, en français).

■ **Autorités**. Cette technologie nécessite la délivrance par des sociétés appelées Autorités de Certification (AC) de certificats de signature électronique.

➔ L'autorité de certification (AC) définit une politique de certification, et la fait appliquer. L'autorité de certification est responsable vis à vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification et donc de la validité des certificats qu'elle émet. Certaines AC sont reconnues par les pouvoirs publics (Ministère des Finances, Minefi).

➔ L'autorité d'enregistrement (AE) vérifie que le demandeur de signature électronique est bien la personne qu'il prétend être, et ce conformément aux règles définies dans la politique de certification. L'autorité d'enregistrement a un rôle essentiel d'identification.

➔ L'opérateur de certification (OC) assure la fourniture et la gestion des certificats électroniques. Son rôle consiste à mettre en œuvre une plate-forme technique sécurisée, et ce dans le respect des exigences énoncées dans la politique de certification. Il assure les prestations techniques, en particulier cryptographiques, nécessaires au processus de certification.

■ **Types de signatures (certificats)**. Il existe aujourd'hui, en droit français, 3 types de signature électronique :

→ La signature électronique (effectuée avec des certificats de classe 1) : elle permet de contrôler l'intégrité du document, mais pas l'identité du signataire (les certificats de classe 1 sont remis selon un processus de contrôle très léger).

→ La signature électronique sécurisée (effectuée avec des certificats de classe 2 et/ou 3) : elle permet de contrôler l'intégrité du document et d'assurer une authentification forte du signataire (par exemple : le Minefi accepte ce type de signature pour les déclarations de TéléTVA). Plus la classe est élevée, plus le lien entre la clé publique établie par le certificat électronique et la personne physique est « certain ».

→ La signature électronique sécurisée PSC (effectuée avec des « certificats qualifiés », voir arrêté du 26 juillet 2004.) : il n'existe pas aujourd'hui d'offres permettant de telles signatures électroniques mais les premiers PSC devraient être certifiés au printemps 2005 (dès approbation du référentiel du COFRAC préparé l'automne dernier avec la DCSSI et l'ADAE).

■ **Exemples**. Les télé-procédures vous imposent de vous identifier ou de signer votre déclaration électroniquement. Dans le cas des télé-procédures, le risque est essentiellement réglementaire ou juridique. Il faut vous conformer aux exigences des procédures de dématérialisation des actes juridiques selon les modalités inscrites dans les textes de lois autorisant les déclarations et échanges administratifs par voie électronique (en principe ces exigences sont clairement indiquées sur le site Internet). Quelques exemples :

→ Télé-TVA est l'une des premières télé-procédures accessibles à l'ensemble des entreprises pour la déclaration de la TVA par voie électronique. Le site du Minefi donne toutes les précisions nécessaires, dont les AC (autorités de certification) agréées.

→ La sécurisation des échanges entreprises/acheteurs publics dans le cadre de la dématérialisation des procédures de commande publique nécessite l'utilisation de certificats, selon des modalités définies par l'entité publique acheteuse.

→ La facturation électronique est maintenant autorisée : elle pourra requérir l'usage d'un certificat de signature électronique sécurisée.

■ **Le Chiffrement** consiste à traiter une information par un procédé mathématique, de sorte que seules les personnes possédant la clé appropriée puissent rétablir, lire et traiter ladite information.

■ **Principe.** Le principe des techniques de chiffrement est d'utiliser un code pour chiffrer les messages et un code pour les déchiffrer. Ces techniques existent depuis l'antiquité (par exemple, Jules César utilisait des messages chiffrés pour communiquer avec ses généraux). En 1976, Diffie et Hellmann inventent le procédé de chiffrement à clé publique. L'idée est que la clé est séparée en deux parties, l'une pouvant être divulguée et l'autre devant rester confidentielle.

■ **Catégories**. Il existe 2 grandes catégories de chiffrement :

■ **Le chiffrement symétrique** (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clef pour le chiffrement et pour le déchiffrement.

→ Il faut prévoir que chacun utilise une clé différente pour communiquer avec chaque correspondant.

→ Le principal inconvénient d'un crypto-système à clefs secrètes provient donc de l'échange des clés : le chiffrement symétrique reposant sur l'échange d'un secret (les clés), se pose le problème de la distribution des clés

■ **Le chiffrement asymétrique** (aussi appelé crypto-système à clés publiques), est basé sur le principe que les clés existent par paires (on parle souvent de bi-clés): une clé publique pour le chiffrement et une clé privée ou secrète pour le déchiffrement.

➔ Ce qui a été chiffré par la clé publique ne peut être déchiffré qu'avec la clé privée et ce qui a été chiffré par la clé privée ne peut être déchiffré qu'avec la clé publique.

➔ Les utilisateurs choisissent une clé aléatoire dont ils sont seuls connaisseurs (il s'agit de la clé privée). A partir de cette clé, les utilisateurs déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

■ **Méthodes de chiffrement**. Dans les échanges électroniques des données, on emploie toute une série de méthodes de chiffrement, comme SSL ou PGP, consistant à crypter les données soit avant, soit pendant leur transfert :

■ SSL est un protocole de transfert de données qui permet de chiffrer l'échange électronique pendant son transfert entre l'expéditeur et le destinataire. Cette forme de transmission cryptée des données est surtout utilisée pour les services bancaires en ligne et pour le commerce électronique, par exemple pour la transmission de données confidentielles (mots de passe, numéros de cartes de crédit) entre un navigateur et un serveur.

■ PGP est un procédé de chiffrement hybride, qui sert à crypter des données au moyen d'une clé publique et à les déchiffrer à l'aide d'une clé privée. PGP est actuellement le système le plus employé pour le chiffrement du courrier électronique.

■ **La Biométrie** est un moyen reconnu comme étant de plus en plus fiable pour vérifier l'identité électronique des personnes mais les textes n'en prévoient pas encore l'usage de manière explicite. C'est donc une technologie dont la montée en charge est à suivre dans les années qui viennent.