

SECURITE LOGIQUE

Chiffrement

LOGI02

Contexte :

Les risques de divulgation et d'altération d'informations, risques d'autant plus graves que les informations sont plus sensibles, sont de plus en plus élevés. Les causes identifiées les plus courantes sont :

- Les vols de micro-ordinateurs et surtout de portables en tous lieux
- Les intrusions et les écoutes à travers les réseaux en général
- Les infections logiques (diffusion de fichiers par les vers ou récupération de données par la technique du Cheval de Troie)
- Les erreurs et les malveillances internes à l'entreprise
- Les nouvelles technologies de stockage miniaturisées (clés USB, smart cards, disques ..)
- Les médias de communication (Bluetooth, Wifi ...)

Objectifs :

Empêcher à l'aide d'un logiciel de chiffrement des données, l'utilisation par des personnes non habilitées, d'informations définies comme sensibles par l'entreprise ou l'organisme.

Recommandations :

Toute information sensible doit être chiffrée sur tout micro-ordinateur, en particulier sur les portables.

Il est souhaitable que l'administration du logiciel de chiffrement soit centralisée :
Un administrateur est donc nécessaire. Il a obligation de conserver les clés en lieu sûr, sous forme chiffrée (ou enveloppe cachetée), et de prévoir une sauvegarde.

Un utilisateur ne doit pas pouvoir créer de clé.

Il est impératif de respecter le cadre légal dans le domaine du chiffrement (par exemple, la longueur des clés utilisées).

Remarques :

Le chiffrement est susceptible de ralentir les performances.
Lors de la première utilisation, le chiffrement des données existantes risque d'être consommateur de ressources (par exemple : base de données sur un serveur).

En général, la cryptographie consiste à chiffrer, signer, authentifier les données.

Se reporter au document du CLUSIF : « Le chiffrement ».

Liens utiles :

Synthèse du cadre légal en matière cryptographique : site de la DCSSI : www.ssi.gouv.fr



Les présentes recommandations ne sauraient mettre en cause la responsabilité du CLUSIF, elles ne présentent qu'un caractère indicatif et ne sauraient prétendre à l'exhaustivité.