SSII ETICSYS

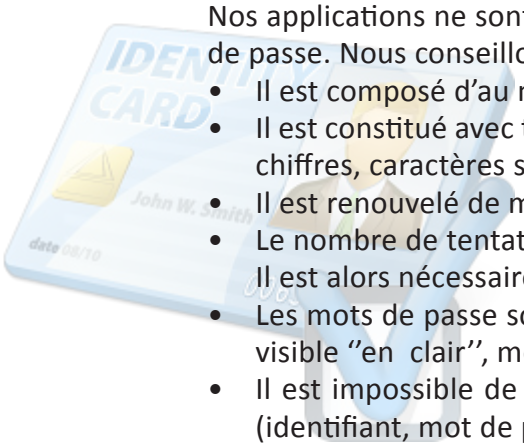
Sécurité

Eticsys est soucieux de la sécurité des solutions informatiques mises à disposition de ses clients. Pour cela nous agissons sur deux axes principaux :

- Le premier, en proposant l'implémentation des mécanismes adéquats dans nos solutions pour assurer et gérer la sécurité de la solution, en fonction des besoins exprimés et des possibilités.
- Le second, en vous conseillant sur les actions à mettre œuvre et les moyens à déployer pour garantir la sécurité de l'environnement informatique de nos solutions dans votre Système d'Information.

Pour ce faire, nous appliquons les « règles de l'art » décrites dans la bibliothèque ITIL pour partie et principalement les recommandations édictées par la CNIL pour la confidentialité des données.

Mot de Passe



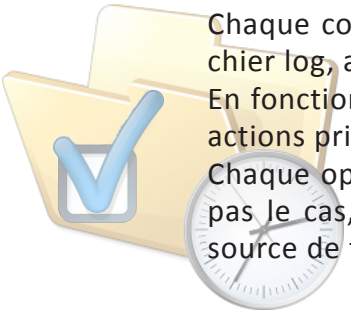
Nos applications ne sont accessibles qu'au travers de la saisie d'un identifiant et d'un mot de passe. Nous conseillons la mise en œuvre des règles suivantes :

- Il est composé d'au moins 8 caractères.
- Il est constitué avec trois types de caractères différents entre : majuscules, minuscules, chiffres, caractères spéciaux.
- Il est renouvelé de manière périodique (au moins 1 fois/an).
- Le nombre de tentative est limité, avec un blocage du compte au bout de 3 tentatives. Il est alors nécessaire pour l'administrateur d'intervenir afin débloquer le compte.
- Les mots de passe sont chiffrés au niveau des mécanismes de stockage et ne sont pas visible ''en clair'', même pour l'administrateur.
- Il est impossible de se connecter plusieurs fois simultanément avec le même couple (identifiant, mot de passe)

Habilitations

Chaque compte d'un utilisateur est associé à un profil définissant les actions qui peuvent être réalisées. Cela permet à l'administrateur de définir les actions qui peuvent être entreprises par un utilisateur possédant un profil donné.
Chaque compte d'utilisateur peut être ou non activé par l'administrateur.

Traçabilité



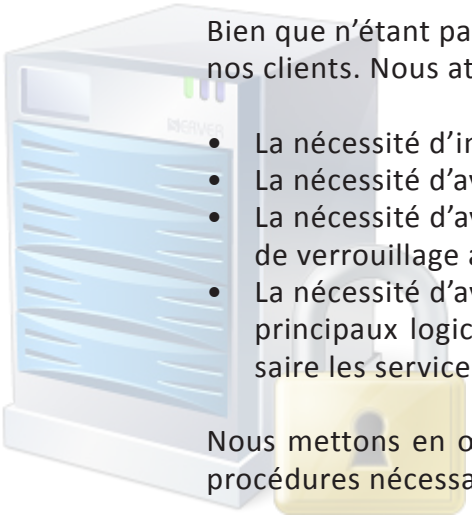
Chaque connexion et déconnexion d'un utilisateur est inscrite dans un journal ou fichier log, ainsi que les tentatives infructueuses.
En fonction du type d'application et du niveau de suivi nécessaire, nous inscrivons les actions principales effectuées par un utilisateur.
Chaque opération est horodatée avec l'heure du serveur. Nous conseillons, si ce n'est pas le cas, de mettre en place un client NTP pour synchroniser le serveur avec une source de temps fiable.

SSII ETICSYS

Données

En cas de besoin, aussi bien pour le stockage que pour l'échange de données, nous implémentons un cryptage des données. Par exemple, lors d'échange de données sensibles avec un ''Web Services'' le protocole SSL est utilisé.
Lors de la mise en place d'une base de données, la connexion y est sécurisée par mot de passe et restriction des accès aux stricts besoins. En cas de nécessité, les données stockées peuvent être cryptées, par exemple avec un hash code type MD5 ou SHA-2.

Postes de travail & Serveurs



Bien que n'étant pas fournisseurs de ces éléments, nous conseillons systématiquement nos clients. Nous attirons leur attention sur :

- La nécessité d'installer des firewalls, individuels et/ou sur l'accès à l'intranet.
- La nécessité d'avoir un antivirus maintenu à jour sur chaque poste.
- La nécessité d'avoir un politique de sécurité incluant pas exemple, la mise en place de verrouillage automatique des postes.
- La nécessité d'avoir une politique de mise à jour des systèmes d'exploitation et des principaux logiciels utilisés sur l'Internet®.La nécessité de limiter au strict nécessaire les services accessibles des serveurs.

Nous mettons en œuvre avec nos clients, dans le cadre de leur politique définie, les procédures nécessaires à la sauvegarde des données de nos applications.

Postes Mobiles

Nos solutions utilisent régulièrement des Postes de Saisie Mobile (PDA durcis). Les communications en WIFI doivent être sécurisées à minima avec un protocole WPA en chiffrement AES (WPA-2).
En cas de besoin de transmission M2M en 3G via un opérateur, nous chiffrons si nécessaire les données au travers du protocole SSL.

Nous bridons systématiquement nos appareils en mettant en place un bureau restreint ''Eticsys''™ qui permet à l'utilisateur de n'accéder qu'aux applications prédéfinies. L'accès à l'ensemble de la machine est verrouillé par un mot de passe spécifique à l'administrateur.

Conclusion

Les divers points exposés dans cette note sont donnés à titre d'informations et qualifie le niveau de sécurité de nos solutions. Dans tous les cas, nous aborderons ce sujet avec vos équipes afin d'intégrer vos contraintes et règles établies.