Complément de la correction de la série de TD n°01

Exercice 03 :

Chaque document relatif à la sécurité s'adresse à un public. Il devrait être écrit de manière accessible. Pour les documents cités dans l'énoncé de cet exercice le public cible est le suivant :

– *le règlement des utilisateurs :* tous les utilisateurs du système informatique, ainsi que le responsable de la sécurité qui élabore ce règlement.

– *le plan de reprise et de continuation* : le responsable de la sécurité ainsi que tous les administrateurs (services de courrier électronique, du serveur Web, etc.) pour l'aspect technique, mais aussi les personnes concernées par la relation clientèle : direction, chargé de communication, etc.

- *Plan de reprise des activités :*
  - Mesures qui visent à rétablir la situation normale
  - Reprise à « froid » → permet un démarrage rapide de l'activité après un sinistre → restauration du système avec les données de la dernière sauvegarde
- *Plan de continuation des activités :*
  - Mesures qui visent à offrir les services critiques pendant le rétablissement
  - Maintenir l'activité en cas de sinistre

– *la politique de sécurité* : le responsable de la sécurité et la direction. Les utilisateurs et les administrateurs peuvent aussi y avoir accès mais ils ne sont pas directement concernés.

Exercice 04 :

On définit ci-dessous les termes proposés.

– Le niveau de sécurité de base (baseline security) représente l'ensemble des mesures de sécurité nécessaires à la protection d'un système d'information contre les menaces usuelles.

– La certification de sécurité atteste qu'un produit donné vérifie des critères définis selon une norme spécifique.

– La politique de sécurité est l'ensemble des règles générales ayant pour but de contrôler et de limiter les risques liés à l'utilisation d'un système d'information.

On donne ci-dessous les objectifs des trois références proposées.

IT Grundschutz-Handbuch (GSHB) : ce manuel concret et technique est un catalogue de menaces et de mesures de sécurité à prendre afin d'obtenir un niveau de sécurité de base, protégeant contre les menaces résultant de l'utilisation standard d'un système d'information. Ce manuel est donc utile afin d'établir un *niveau de sécurité de base*.

ISO 27001 (ancien ISO 17799) : Ce standard permet de définir une *politique de sécurité* (voir le cours)

Common Criteria (ISO 15408) : cette norme internationale définit des critères de sécurité permettant d'évaluer de manière homogène des produits liés à la confidentialité, à l'authenticité et à l'intégrité des données en vue de leur attribuer une *certification*