STYLES

EXERCICE A

Charger le fichier "**Exa-styles.doc**" et modifier les styles "**CorpsText**", "**Evidence**", "**Titre 1**", "**Titre 2**" et "**Puce1**" de manière à ce qu'ils ressemblent à peu près au modèle ci-dessous.

Titre1

UN IMPÉRATIF : LA SÉCURITÉ

CorpText

En matière de sécurité, pas de prêt-à-porter. Chaque entreprise s'expose (souvent sans le savoir) à des risques qui lui sont propres. Les solutions ne peuvent donc être individuelles. C'est l'une des leçons que l'on peut tirer de cette dernière décennie.

Evidence

Les pertes déclarées aux compagnie d'assurance comme consécutives à un sinistre informatique se sont élevées à 8,1 milliards de francs en 1988. Voici à l'heure actuelle la seule donnée statistique reconnue disponible en France. Elle laisse craindre que la vulnérabilité réelle ne soit plusieurs fois plus importante.

Titre2

PARER À UN ACCIDENT GRAVE OU À UN SABOTAGE

La disposition permanente, ou dans un délai très bref, d'une formule de backup est un moyen physique d'assurer la survie d'un système d'information contre les diverses menaces qui le guettent. En permettant la restauration rapide du système sur des bases saines, le backup est avant tout prévu pour parer à un accident grave ou à un sabotage physique.

Il faut aussi signaler les logiciels de contrôle d'accès logique, qui obligent tout utilisateur à s'identifier avant d'accéder au système et qui réservent cet accès aux seules personnes dûment autorisées.

DES LOGICIELS POUR CONTRÔLER L'UTILISATEUR

Pour renforcer ce contrôle d'accès et protéger des données de haute sensibilité, il existe aujourd'hui des logiciels de gestion de base de données sécurisés. Il s'agit de logiciels susceptibles de gérer et de contrôler le comportement de l'utilisateur à l'intérieur même du système.

Puce1

- Associée à un module de contrôle, une base de données de sécurité n'autorise à l'utilisateur de n'accéder qu'aux seuls fichiers ou programmes qui lui sont officiellement attribués.
- En général, de tels logiciels effectuent en permanence un relevé de l'ensemble des opérations effectuées par les utilisateurs. Ce relevé est conservé à l'abri de toute intervention indésirable.
- En sécurité, il n'y a pas de solutions miracles. Il faut appliquer une méthodologie efficace et approprie
- La sécurité est une chaîne. La faiblesse d'un seul maillon peut tout remettre en question.

EXERCICE B

Charger le fichier " **Exb-styles.doc**" et créer les styles "**Titre**", "**Rubrique**", "**Evidence**"et "**Encadré**". En formatant ces styles, faire en sorte que le document ressemble à peu près à l'exemple ci-dessous.

Rappel : F4 répète la dernière opération !!

titre **QUELS RISQUES ?**

Dans le cas où un réseau de communications est utilisé, on peut recenser les principales menaces suivantes :

rubrique MODIFICATION DE DONNÉES

évidence *PENDANT LEUR TRANSMISSION, PAR EXEMPLE, LORS DE LEUR TRANSIT DANS UN NŒUD DE COMMUNICATION, OU ENCORE AVANT LEUR ÉMISSION.*

MASCARADE OU USURPATION D'IDENTITÉ

CONSISTANT À SE FAIRE PASSER POUR UN AUTRE UTILISATEUR DU SYSTÈME EN UTILISANT SON IDENTIFIANT ET SON MOT DE PASSE ET EN S'EN ARROGEANT LES DROITS.

TRAPPES

PROGRAMMES DESTINÉS À PROVOQUER UNE DÉFAILLANCE DU SYSTÈME, DE MANIÈRE À OBTENIR L'ACCÈS OU À PERMETTRE LA MODIFICATION OU LA DESTRUCTION DES DONNÉES.

BOMBES LOGIQUES

PROGRAMMES PROVOQUANT LA DESTRUCTION DE DONNÉES LORSQU'UNE CERTAINE CONDITION EST RESPECTÉE (EX. : LORSQU'UNE DATE DÉTERMINÉE EST ATTEINTE).

VIRUS

PROGRAMME SE REPRODUISANT ET ENGENDRANT DES DYSFONCTIONNEMENTS DU SYSTÈME (EX.: SATURATION DE LA MÉMOIRE CENTRALE).

VERS

PROGRAMME SE DÉPLAÇANT DANS LE SYSTÈME ET PRODUISANT DES DÉGÂTS SUR SON PASSAGE.

SALAMIS

UTILISATION DES ERREURS D'ARRONDIS DANS LES CALCULS FINANCIERS.

QUELLES PROTECTIONS ?

CONFIDENTIALITÉ

encadré

Propriété qui assure la tenue secrète d'informations avec accès pour les seuls utilisateurs autorisés.

INTÉGRITÉ

propriété qui assure que des informations sont identiques en deux points, dans l'espace ou dans le temps.

DISPONIBILITÉ

Aptitudes d'un système à remplir des fonctions dans des conditions prédéfinies d'horaires, de délais, de performances.

AUDITABILITÉ

contrôle du bon fonctionnement d'une fonction.

NON_RÉPUDIABILITÉ

impossibilité pour une entité de nier avoir reçu ou émis un message (suppose l'authentification).