Exercice 3.1
Étude de cas « centre d'hébergement »

Une équipe de 15 personnes est chargée, dans un grand centre d'hébergement informatique (nommé CH dans la suite de l'énoncé), de la supervision et de l'exploitation des systèmes informatiques.

Les clients de ce centre sont des entreprises diverses qui, n'ayant pas les compétences en interne, ont décidé de lui confier l'hébergement de leur application. De par la diversité des entreprises clientes, les besoins de sécurité des applications hébergées sont très variables et on trouve pour chaque critère de sécurité (disponibilité, intégrité, confidentialité) au moins une application qui possède un besoin de sécurité très élevé.

Les missions de l'équipe sont les suivantes :
- concevoir les architectures réseau, système et supervision
- installer les équipements, les systèmes d'exploitation et les applications
- maintenir les systèmes (mises à jour de sécurité, etc.)
- superviser l'ensemble du système et corriger les écarts constatés
- répondre aux demandes des clients et réaliser le suivi de ces demandes
- documenter le système

Les valeurs de l'équipe sont les suivantes :
- la réactivité
- la disponibilité des applications
- une bonne connaissance et un bon suivi des clients
- la capacité à bien conseiller les clients

Lors d'une itération du cycle de Deming, l'équipe a pris conscience de l'importance d'améliorer encore l'efficacité des deux sous-processus suivants :
- répondre aux demandes clients et réaliser un suivi de ces demandes
- documenter le système

Il a donc été décidé de faire une appréciation des risques détaillée sur ces deux sous-processus. La suite de cet exercice concerne ce périmètre et cette action.

Description du périmètre étudié

Deux outils sont à la disposition de l'équipe pour réaliser la mission concernant ces deux sous-processus :
- GT : Un gestionnaire de tickets pour gérer le suivi des demandes clients.
- BC : Une base de connaissance de type « Wiki » pour gérer les fiches de documentation du système (une fiche par sujet)

GT est une application Web, permettant de saisir à l'intérieur d'un « ticket » :
- la demande
- des informations sur le client
- l'ensemble des échanges ayant permis de traiter cette demande
- des pièces jointes éventuelles

Les clients peuvent créer des tickets de deux manières :

- directement dans l'application Web : www.ch.fr après authentification
- ou en envoyant un courrier électronique à l'adresse « ticket@ch.fr »

On donne les informations techniques suivantes sur l'architecture :

- Le protocole HTTPS n'est pas utilisé.
- Une authentification type « utilisateur/mot de passe » est utilisée.
- Les données de GT et BC sont stockées dans une base de donnée MySql installée sur le serveur SERV1.
- Il existe une passerelle entre GT et BC. Les tickets intéressants peuvent alimenter la base de connaissance.
- Les courriers qui alimentent GT transitent par un serveur de messagerie du centre utilisant Postfix et installé sur le serveur SERV2. Ce serveur n'est pas redondé. Aucun mécanisme anti-spam ne lui est associé.
- Tous les serveurs utilisent le système d'exploitation Linux.

On donne les informations complémentaires suivantes :

- Afin de garantir la meilleure réactivité, tout le personnel du centre doit pouvoir accéder 24 heures sur 24 et 7 jours sur 7 aux applications GT et BC depuis n'importe quel endroit par Internet.
- Malgré la politique de sécurité interdisant ce type de pratique, des informations à caractère confidentiel (secret, mot de passe) sont régulièrement retrouvées (pendant les phases d'audit) dans les fiches du Wiki et dans les tickets !

➔ Description du travail à réaliser page suivante...

Travail à effectuer

Question n°1

Grâce à l'énoncé ci-dessus, réaliser l'inventaire des actifs supports et des actifs primordiaux. Pour chaque actif support, indiquer sa catégorie. Pour chaque actif primordial, indiquer s'il s'agit d'une information ou d'un processus.

Dans quelle étape de la démarche ISO 27005 réalise-t-on cette tâche ?

Question n°2

On rappelle la définition d'un **événement redouté** : « Il s'agit d'un scénario générique représentant une situation crainte par l'organisme. Il s'exprime par la combinaison des **sources de risque** susceptibles d'en être à l'origine, d'un **actif primordial**, d'un critère de sécurité, du **besoin de sécurité** concerné et des **impacts** potentiels. »

Identifier deux événements redoutés par CH sur le périmètre étudié. Vous êtes libre de choisir vos sources de menace et vos impacts.

Question n°3

Relever une liste de vulnérabilités sur le périmètre étudié.

Question n°4

Identifier deux scénarios de menaces (combinaison des sources de risque, des menaces / modes opératoire, des vulnérabilités exploitables et des actifs supports concernés) sur le périmètre étudié.

Question n°5

Identifier deux risques concernant le périmètre étudié. Faire apparaître clairement les sept composantes de chaque risque.

Pour aller plus loin…

Pour chacun des risques identifiés à la question n°5 ci-dessus, proposer des mesures de sécurité à mettre en place pour réduire le niveau de ces risques.