Sécurité - TD 3

12 décembre 2018

1 Exercice 1 : Principe de l'ISO 27001

1.1 Quelles sont les différentes étapes d'une appréciation du risque ?

— Identification des risques (vulnérabilités, conséquences, menaces, actifs)
— Estimation des risques (Estimation conséquences, probabilité d'occurrence, impacts)
— Évaluation du risque

1.2 Question 2

— Vulnérable car connecté au réseau interne et non mis à jour
— Toute personne malintentionnée ayant accès au réseau de l'entreprise + wifi ouvert au public s'il existe
— Pas de confidentialité, modification ou suppression de données (DIC)
— Installer les mises à jour de sécurité
— Régression de service dû aux mises à jour. Le serveur est peut être déjà infecté
— Il faut effectuer une analyse du serveur pour désinfection. Vérifier la compatibilité du matériel (Serveur de test).

1.3 Question 3

— Accès physiques
— Les utilisateurs
— Disponibilité, Intégrité, Confidentialité (DIC)
— Mettre des porte et des serrures
— Mauvaises gestion des mesures de sécurité misent en place
— Durcir l'accès (alarme si la porte reste ouverte, etc...)

1.4 Question 4

— Accepter
— Réduire (prendre des mesures)
— Refuser (supprimer le service)
— Transférer (sous-traiter)

1.5 Question 5

Oui, si le risque à un impact faible et une probabilité d'occurrence faible, il peut être définis comme acceptable.

1.6 Question 6

Malgré les mesures de sécurité misent en place, certaines peuvent être réduites mais pas évitées totalement.

1.7 Question 7

Elle doit donner son approbation pour accepter ou refuser le risque résiduel.

1.8 Question 8

— Objectifs de sécurité sélectionnés
— Mesures de sécurité retenues avec justification
— Mesures de sécurité effectivement mises en place
— Mesures de sécurité non retenues avec justification

1.9 Question 9

Elle sert à vérifier que l'on a rien oublié.

1.10 Question 10

Simplification de l'audit.

1.11 Question 11

Voir chapitre 7.2 + 4.2.3b du document de la certification ISO 27001.

1.12 Question 12

Permet de certifier un SMSI.