Ugo

BEMBEN

2022

TP TD Cybersécurité

1) **Protection en temp réel :**

Cette configuration permet de d'identifier et d'empêcher l'installation de programmes malveillants sur son appareil

Notification de protection contre les virus et menaces :

Cette configuration permet de d'être avertis des activités récentes

Protection dans le cloud :

Cette configuration permet d'offrir une protection renforcée et plus rapide grâce à l'accès aux données de protection

Contrôle des applications et du navigateur

Cette configuration permet de protéger les applications
qui ne sont pas reconnus à partir d'Internet

Connexion entrante

Cette configuration permet de bloquer les connexions entrantes sur un réseau prive.

Mise à jour Windows

Cette configuration va permettre de mettre à jour régulièrement le système d'exploitation automatiquement pour éviter que le système d'exploitation soit vulnérable.

1. Identifiez les configurations à modifier pour garantir la sécurité du SI.

Pour garantir la sécurité du SI il faut activer :

-la Protection en temps réel,

-les notifications contre les virus et menaces

-activer le contrôle des applications et du navigateur

-l'installation automatique des mises à jour.

2. Voici quelques outils qui pourraient vous être utiles : pare-feu, filtre de courrier indésirable, correctifs et mise à jour, logiciel anti-espion, bloquer de fenêtre intempestive, antivirus.

Vous citerez différents outils utilisables sur le SI et préciserez le rôle de chacun d'eux.

Sur le SI nous pourrions utiliser :

- Un pare-feu qui permettra d'autoriser ou d'interdire un accès à un ou des services et contrôler les applications et les flux de données
- Un anti-spam qui permettra de bloquer le spam de mail, de messages et des appels.
- Filtre de courrier indésirable qui permettra de filtrer les mails indésirables

- Logiciel anti-espion qui permettra de de se protéger contre les logiciels malveillants
- Les antivirus qui permettront d'éviter et de prévenir des virus qui pourront endommager votre ordinateur.
- Le proxy qui permet de vérifier et faciliter les échanges entre les hôtes

3. Vous préparerez une machine cliente Windows 10 avec les outils que vous jugez nécessaires à la sécurité du SI.

4. Précisez si l'ensemble de ces outils est nécessaire ou si certains peuvent être ignorés.

Pour un maximum de sécuriter sur le SI je conseillerai de utiliser tout les logiciel citer au dessus pour ne prendre aucun risque car on ne sais pas comment vont si prendre pour vous pénétré les Hacker

5. Déterminez l'outil qui répond le mieux à la demande de votre DSI. Justifiez votre réponse

Il est préférable de choisir l'OpenDNS Home Internet Security car il va permettre de bloquer des catégories complètes sans le faire manuellement et nous pouvons également changer les catégories manuellement selon les choix du DSI pour pouvoir sécuriser tous les appareils connectés au réseau, donc on remarque un gain de temps comparé au Proxy switcher du fait de ne pas configurer tous les sites.