Documentation du projet 3PROJ

Réalisé par :
BERRADA Yahia

SOMMAIRE

1) Politique de sécurité

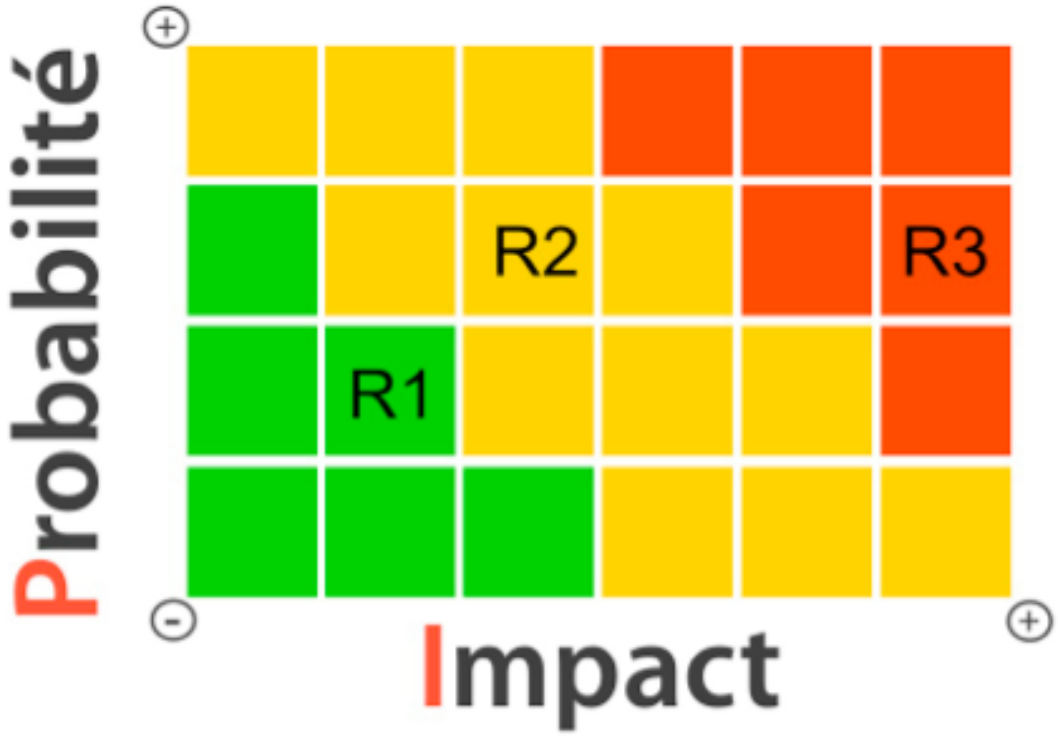
a. Identification des risques

Notre entreprise étant dans le domaine de la santé, elle est sujette à différentes attaques possibles, parmi celles-ci se trouvent :

- Vol d'informations
- Attaques DDoS ou DoS
- Man in the middle
- Logiciels malveillants
  - Chevaux de Troie
  - Ransomwares
  - Spywares
- Phishing
- Vishing
- Attaque brute-force

b. Méthodologie et outils d'analyse des risques

La matrice gravité/probabilité permet de mesurer les degrés de gravité et de probabilité de situations non désirables.
Cette méthode s'utilise avec la matrice ci-dessous en attribuant un score de 1 à 4 pour la gravité et pour la probabilité.
Ce qui nous permettra de voir où le risque se situe, dans la case verte, orange ou rouge.



La case verte signifie que le risque est négligeable, l'orange que le risque est gérable et le rouge dangereux.

c. Politique de sécurité IT

La politique de sécurité dans un centre de santé, comme un hôpital par exemple, est une chose très critique. Énormément d'informations sensibles, personnelles, confidentielles sont détenus dans les systèmes d'informations hospitaliers.

C’est pour cela, qu’il faut définir une politique de sécurité.

Voici donc un exemple de politique de sécurité en utilisant la roue de Deming. Cet outil permet de proposer un processus simple et efficace qui s’applique à de nombreuses problématiques.

Les différents points illustrés dans la roue de Deming seront étudiés dans cette documentation.

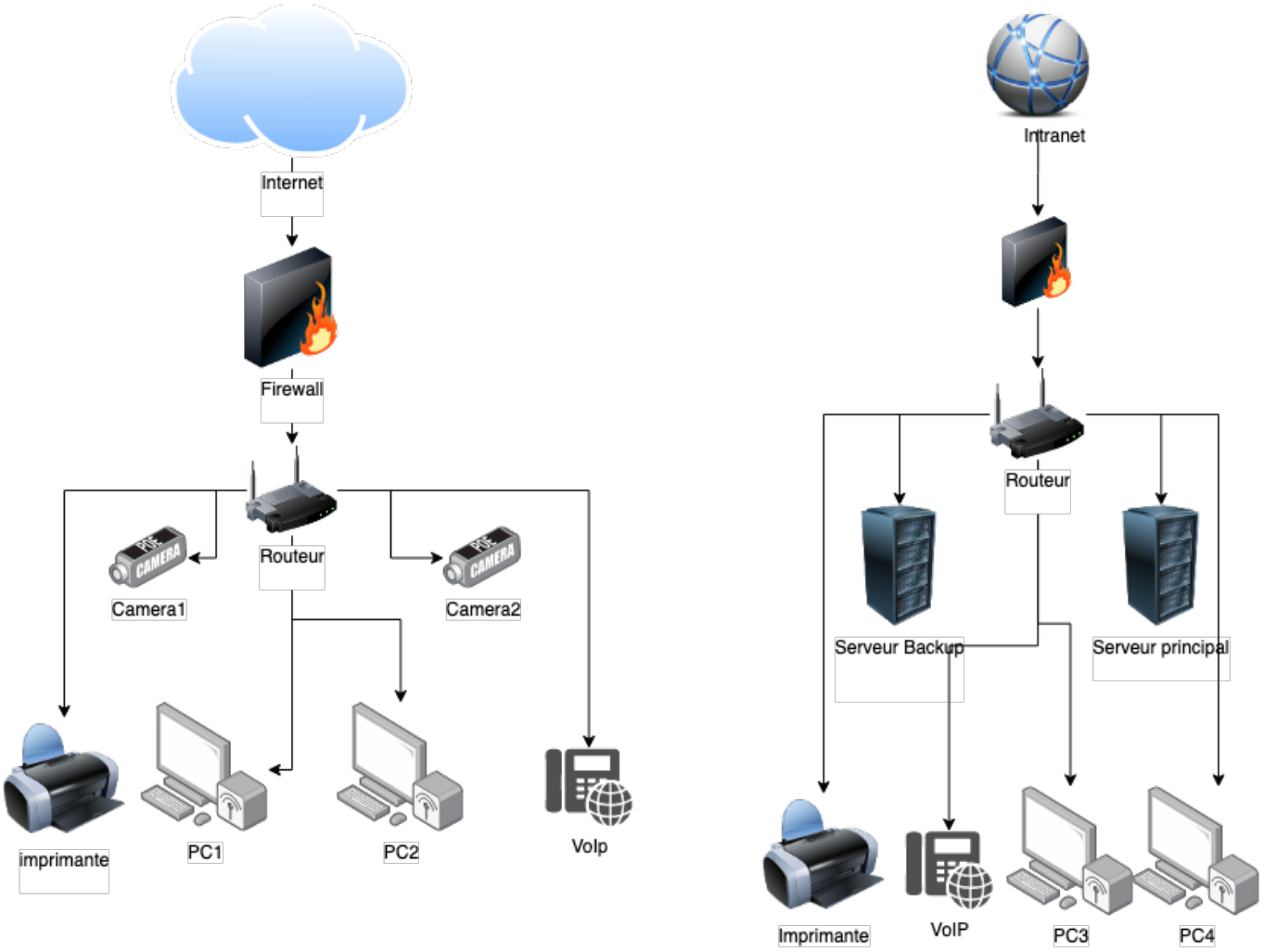
2) Analyse du matériel et solutions existants

a. Registre des éléments du système d'information

Le SI hospitalier comprend :

- Internet
- Intranet
- Ordinateurs
- Imprimantes
- Serveurs
- Caméras
- VoIP
- Firewall
- Base de données
- Service de backup

b. Carte des éléments du système d'information



Dans cette carte des éléments du SI, on peut apercevoir une partie des équipements connectés au réseau internet et une autre partie connectée au réseau intranet.

3) Analyse des risques informatiques

a. Définition des types de risques et d'attaques

Vol d'information :

Le vol d'information peut être très critique pour les entreprises et principalement pour les entreprises de santé comme les cliniques, hôpitaux qui peuvent dévoiler les informations personnelles des clients, des employés et de de toute la structure.

La contre-mesure de cette menace est tout d'abord de sensibiliser les directions au risque SI, ensuite d'établir un schéma des applications connectés au service SI et de cartographier les traitements mis en œuvre par service. Il faut également analyser la conformité de chaque traitement, tenir à jour un registre des activités de traitements, contrôler les contrats passés avec des prestataires externes, effectuer des tests d'intrusions sur les applications sensibles, sensibiliser le personnel sur les risques SI et lancer des actions d'ingénierie sociale.

Attaque DDoS ou DoS

Tout d'abord, une attaque DDoS est le fait que plusieurs machines « zombies » aient été infecté afin d'attaquer simultanément un serveur ou un site web pour le saturer de connexion et le faire planter.
L'attaque DoS quant à elle, peut être effectuée par n'importe qui sans avoir besoin de machines infectés.

La contre-mesure de l'attaque DoS est simple contrairement à l'attaque DDoS, car vu qu'il ne s'agit que d'un seul attaquant, il suffit de bloquer son adresse IP sur le serveur. Contrairement à l'attaque DDoS qui est plus difficile à détourner, et qui pour s'en protéger, l'entreprise doit opter pour des hébergements spécialisés qui résistent à la surcharge de bande passante et qui permettent d'isoler les attaques.

Man in the middle

Le Man in the middle est une attaque qui consiste à un attaquant de pouvoir intercepter les communications qui peuvent être établis sur une connexion internet. L'attaquant doit donc pouvoir être connecté au même réseau wifi que la cible pour intercepter ses communications.

La contre-mesure de cette attaque est tout d'abord de vérifier qui peut avoir accès a votre connexion internet ensuite de vérifier que l'on navigue sur des sites web « https », ce qui permet de chiffrer le trafic et d'être en mesure également d'utiliser un VPN pour chiffrer l'ensemble des requêtes effectuées sur internet.

Logiciels malveillants

Il existe différents types de logiciels malveillants, parmi ceux-ci, les plus connus sont : les chevaux de Troie ou trojan, les ransomware et les spywares.
Les trojans consistent à infecter votre machine à travers une application qui semble honnête mais qui en réalité injecte du code malveillant une fois que l'application a été lancé.
Les ransomware consistent à bloquer votre machine et crypter toutes les données qui s'y trouvent jusqu'à ce que vous décidiez de payer l'attaquant pour qu'il vous redonne l'accès à votre machine.
Les spywares sont des applications espionnes qui peuvent récupérer des données sur ce que vous taper sur votre clavier par exemple.

La contre-mesure principale des logiciels malveillants est bien évidemment de faire attention à ce que l'on télécharge et d'utiliser des logiciels crées par des éditeurs de confiance ou développer par des sociétés de confiance. Il faut également posséder d'un anti-virus de bonne qualité qui vous permettra d'effectuer des scans régulièrement.

Phishing

Le phishing consiste à tromper une personne en usurpant l'identité d'un site web afin de récupérer les données de la victime qu'elle aurait pu saisir dans le site réel, comme par exemple des informations de connexion pour un service bancaire.

La contre-mesure de cette menace est de bien faire attention à l'adresse du site en question, aux emails que l'on reçoit et aux liens douteux qui peuvent nous être envoyé.

Vishing

Le vishing est le même principe que le phishing sauf que ce dernier utilise le moyen de communication téléphonique afin de vous soustraire des informations.

La contre-mesure de cette menace est de faire attention aux appels que l'on reçoit afin de ne pas tomber dans le piège d'un attaquant, et de ne pas donner d'informations trop sensibles par voie téléphonique lorsque l'on n'est pas sûr de la personne qui vous appel.

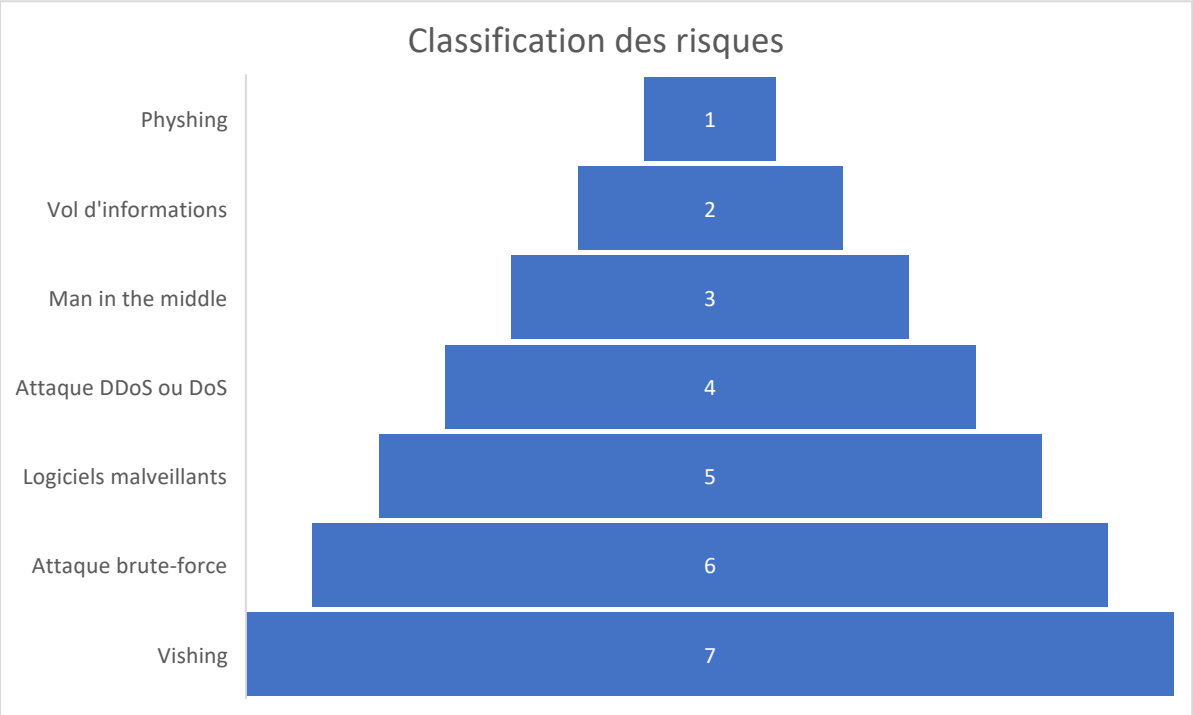
Attaque brute-force

L'attaque brute-force consiste à tester des centaines voire des milliers de combinaisons afin de trouver les mots de passes pouvant permettre une authentification sur des services comme Facebook, boite email, routeur wifi etc.

La contre-mesure de cette attaque est tout simplement d'utiliser des mots de passes d'un niveau de sécurité suffisant pour ne pas permettre à l'attaquant de le trouver. Les spécialistes recommandent des mots de passes d'au moins 10 caractères contenant majuscules, minuscules, chiffres et caractères spéciaux.

b. Classification des risques et des attaques

Voici une classification des risques et attaques énoncées.



4) Moyens nécessaires pour la réduction des risques

a. Mise en place des règles de détections d'intrusions

Les règles de détections et d'intrusions permettent de repérer des activités anormales ou suspectes sur une partie analysée. Elles permettent également de détecter les attaques et de se défendre avant qu'elles ne puissent causer des dommages.
Ces règles vont se baser sur :

- L'action
- Les protocoles à filtrer
- Les adresses IP source et destination
- Les numéros de ports
- L'intégrité des données
- L'authentification forte
- Le firewall
- La gestion du trafic
- La gestion des comptes privilèges

b. Établissement des règles de défense

Les règles de défenses permettent de pouvoir se sécuriser le plus possible face aux attaques probables que dont l'entreprise peut être victime.
Voici dont une liste de règles qu'il convient de respecter :

- Mots de passes de qualité
- Logiciel et système d'exploitation mis à jour
- Backup régulier

- Désactiver des composants non utiles
- Ne pas cliquer sur n'importe quel lien
- Contrôler la diffusion d'infos personnelles
- Naviguer sur internet prudemment
- Ne pas naviguer avec des comptes admin

c. Nettoyage des éléments infectés

Le type de programme malveillant le plus courant est le virus qui peut être copié lui-même d'un système à un autre et qui infecte chaque ordinateur au passage. Lorsqu'un virus a infecté le système d'une entreprise, il peut supprimer ou corrompre des dossiers, voler des données ou même endommager le matériel informatique. Il peut provenir de pièces jointes à un courriel, de téléchargements d'un site Web ou de disques infectés utilisés par plusieurs personnes.

C'est donc pour cela qu'il faut régulièrement scanner les différents éléments de son ordinateur afin de supprimer et de nettoyer les éléments infectés pour que ces derniers ne soient pas en mesure de contaminer d'autre documents souvent critiques pour l'entreprise.

Il faut donc se munir de logiciel antivirus, de pare-feu, d'anti-spyware afin d'essayer au mieux de rester en sécurité.

d. Règles de backup

La sauvegarde est un élément un essentiel pour toute entreprise car elle permet en cas de panne matériel ou d'attaque de garder les informations dont elle a besoin et elle dispose pour travailler.

Souvent, les éléments les plus importants à être sauvegardés sont les données utilisateurs, donc la base de données. Aussi, les fichiers, documents, logs de l'entreprise ont vocation à être sauvegardés afin de ne pas les perdre.

Il faut donc planifier régulièrement des sauvegardes du système sur un ou plusieurs serveurs externes et non reliés à ceux de l'entreprise.

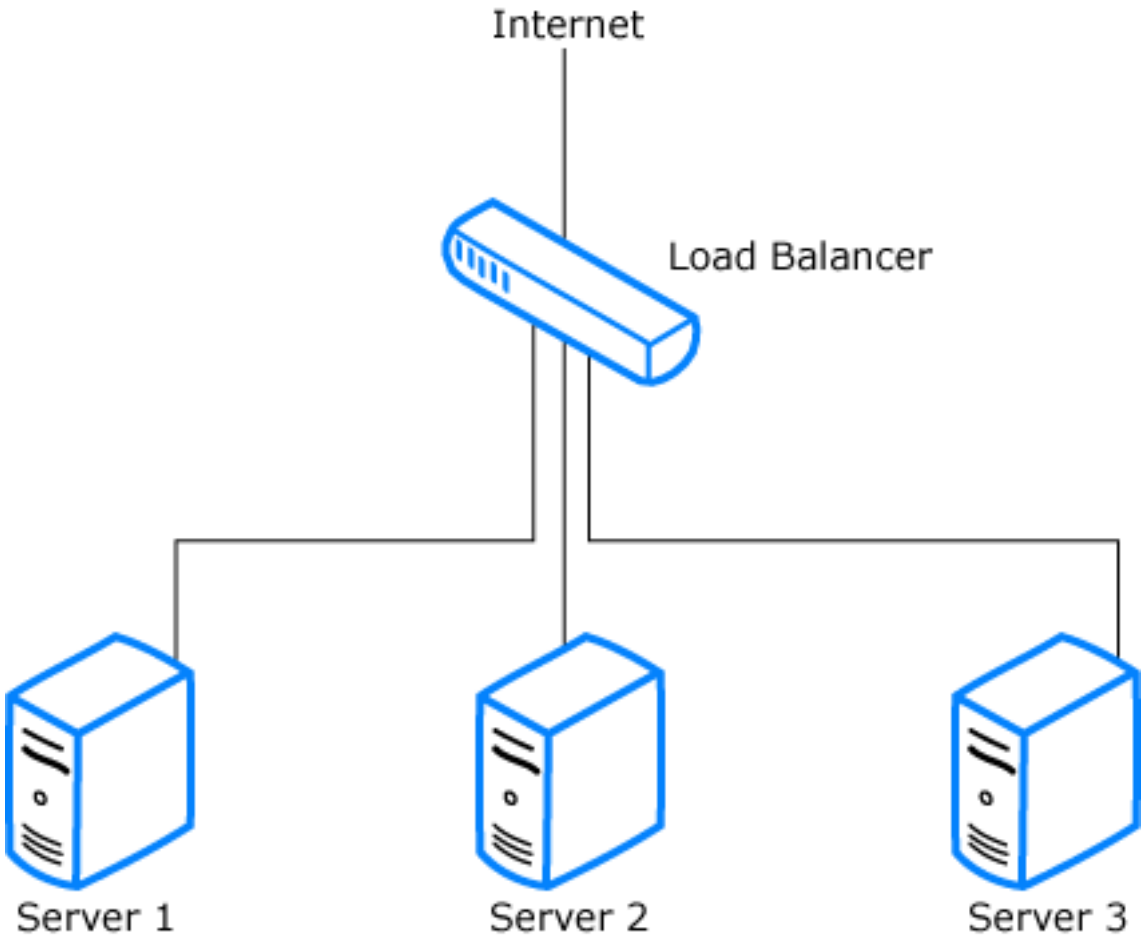
Étant donné que le système de santé dispose d'informations sensibles et critiques qui ne peuvent pas se permettent de se perdre, il faut planifier quotidiennement une sauvegarde à une heure de faible trafic réseau.

e. La garantie de la disponibilité des informations

La disponibilité des informations permet en cas de panne par exemple, de pouvoir continuellement avoir accès à nos données et y effectuer des traitements de mise à jour, suppression, édition, ajout.

Pour cela, l'entreprise doit disposer d'un système de cluster qui va dupliquer le contenu des disques durs sur différents serveurs de l'entreprise et sur le cloud de manière sécurisé afin de pouvoir garantir le système d'accès de données notamment pour le service de santé.

Voici une petite illustration de ceci :



5) Les procédures appropriées et les contre-mesures

Cette partie sera traitée en fonction des procédures mises en place pour la partie technique de ce projet.

a. Définir les procédures pour automatiser les détections d'attaques

Au niveau de la plateforme du serveur, dès qu'une attaque est émis par le client, le serveur détecte automatiquement la menace et affiche dans la partie Monitoring de l'application l'élément attaqué ainsi que dans la partie administration du Monitoring, les différentes statistiques relatifs à cette attaque tels que : l'attaque, la section concernée, la date, l'IP de l'attaquant.

A chaque détection d'attaque, celle-ci est enregistré dans les logs de de la base de données afin de garder une traçabilité et ainsi que dans un fichier Json qui pourra être lu et parcouru par l'algorithme d'intelligence artificielle réalisé.

b. Alertes par type d'attaque

Il y a principalement 4 alertes au total, une pour chaque rubrique de protection, à savoir : protection de la base donnée, protection du serveur, protection backdoor, protection des utilisateurs.

Toutes ces alertes possèdent 2 statuts possibles, soit le statut en online soit le statut offline. Ces 2 statuts permettent de représenter graphiquement les sections attaquées depuis le monitoring afin d'avoir une vue claire sur ce que le serveur subit actuellement.

c. Backup de récupération

Le backup de récupération permet de sauvegarder toutes les données de la base de données pour que ceux-ci ne soient pas totalement perdu en cas d'une attaque contre la base de données.

Le script de backup réalisé permet de sauvegarder la base de données dans le répertoire de ce dernier et pourra donc être importé si besoin.

Cette sauvegarde contient les données des utilisateurs, des sections, des historiques d'attaques, des documents enregistrés par les utilisateurs.

d. Base de données des types d'attaques

Le serveur contient 4 types d'attaques répertoriés dans la base de données qui sont : protection des données, protection backdoor, protection du serveur, protection de la base de données.

Ces types d'attaques sont principalement vulnérable aux attaques backdoor, DoS, données et utilisateurs.

6) Programme développé

a. Manuel utilisateur

Voir manuel utilisateur.pdf ci-joint.

b. Manuel technique

Voir manuel technique.pdf ci-joint.