Analyse de risques

CABINET MEDICAL

BODSON Fabrice
COLLIGNON Thomas
THITEUX Lucas

MASI 2022 - 2023

Table des matières

1. Contexte du cabinet médical

1.1 Contexte

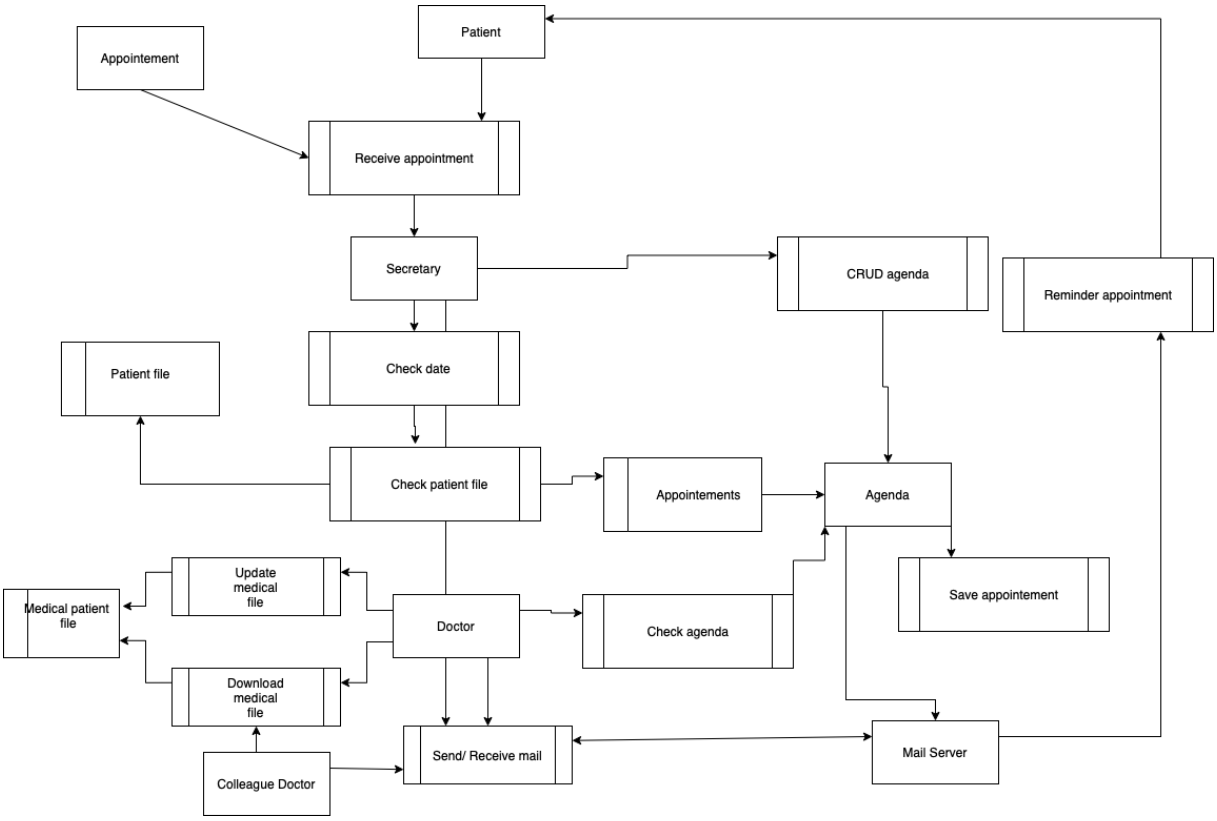
Le cas qui nous a été attribué était un petit cabinet médical. Nous avons imaginé un cabinet médical dans lequel il y aurait un médecin ainsi que sa secrétaire.
La secrétaire aurait la tâche de gérer la prise de rendez-vous, la gestion des informations de contact des patients (adresse, numéro de registre national, …) et la gestion de l'agenda du médecin. Ces informations seraient stockées dans l'ordinateur de la secrétaire. Le médecin n'aurait cependant qu'un accès en lecture à son agenda.
Nous avons imaginé que la gestion du dossier médical des patients serait fournie par une plateforme externe au cabinet. Le médecin ne pourrait que télécharger une copie du dossier médical d'un patient et devrait uploader une nouvelle version sur la plateforme en cas d'ajout d'informations (versioning). Grâce à ce système, les dossiers médicaux ne seraient donc stockés que temporairement dans le cabinet médical.
Lorsque le médecin rencontre un cas complexe, celui-ci pourrait contacter un confrère pour avoir un avis extérieur. Grâce à l'externalisation du dossier médical des patients, le confrère pourrait accéder en lecture au dossier des patients du cabinet.
Pour contacter celui-ci, le médecin utiliserait un serveur mail hébergé localement dans le cabinet médical. Le médecin pourrait également utiliser celui-ci pour contacter la secrétaire. Quelques jours avant une consultation, ce serveur enverrait sur la demande de l'agenda un mail de rappel au patient.
Enfin, si notre cas n'était pas assez complet, nous avons imaginé plusieurs choses à ajouter. Nous pourrions ajouter une plateforme web hébergée dans le cabinet qui permettrait aux patients de réserver leurs rendez-vous en ligne. Nous avons également imaginé un accès au réseau de cabinet par les patients via la mise en place d'une borne d'accès Wi-Fi dans la salle d'attente ou via le paiement d'une place de parking.

1.2 User-story

Le patient téléphone à la secrétaire pour prendre un rendez-vous auprès de son médecin. Cette dernière consulte que la date est disponible dans l'agenda. Si oui, elle consulte ensuite ses informations personnelles avant de l'encoder dans l'agenda. Si non, le patient doit proposer une nouvelle date. Le patient se verra recevoir un rappel de rendez-vous transmis via le serveur mail.

Lorsqu'il commence sa journée, le médecin consulte son agenda pour voir quels patients il recevra et dans quel ordre. S'il a un imprévu, il doit demander à la secrétaire de modifier un rendez-vous, car il ne peut pas le faire directement.
Lors d'une visite, le docteur peut télécharger le dossier médical depuis une plateforme externe. Il peut ajouter une mise à jour, de sorte que les anciennes versions soient toujours disponibles pour les autres médecins (pas de suppression).
Si le médecin souhaite une expertise complémentaire, il peut contacter un de ses collègues en lui envoyant un mail. Ce dernier peut répondre à ce dernier à travers le serveur mail. Il devra cependant accéder au dossier médical du patient par lui-même.

1.3 DFD



2 Méthode EBIOS-RM 2018

2.1 Atelier 1 : Cadrage et socle de sécurité

Maintenant que les flux et les différents acteurs intervenants avec le système, il est possible de passer à l'analyse de risque. La première étape est de définir qui a la charge de quoi face à certaines tâches. C'est dans cette matrice RACI que nous avons défini cela.

2.1.1 Matrice RACI

Voir Figure 1 dans les Annexes.

Les différentes tâches que nous avons pu rassembler sont les suivantes, avec leurs rôles :

- Gestion des rendez-vous :
  La personne **responsable** du bon fonctionnement des rendez-vous est le **docteur**, car c'est lui qui contrôle si c'est correctement encodé et qui est **informé** des RDV pris. Si la gestion des rendez-vous n'est pas correctement faite, alors il aura du mal à travailler et à s'organiser.
  La **secrétaire** est la personne en charge de **réaliser** la gestion des rendez-vous, c'est-à-dire que c'est elle qui s'occupe de prendre les rendez-vous des patients, de les supprimer ou de les modifier.
  Le **patient**, lui, doit **communiquer des informations** comme une date de disponibilité à la secrétaire afin d'organiser le rendez-vous.

- Gestion des informations de contact des patients :
  La **secrétaire** a la **responsabilité** des informations de contact des patients car c'est elle qui communique eux concernant les rendez-vous. Elle est aussi la personne qui **effectue** des modifications ou des ajouts pour les nouveaux patients.
  Le **patient** est à nouveau **consulté** afin de fournir les informations nécessaires.

- Gestion de l'agenda :
  L'agenda est **supervisé** par le **docteur** et celui-ci est **informé** lorsqu'il y a un changement. Il fait savoir à la **secrétaire** ce qu'elle doit **modifier** s'il arrive qu'il soit absent un jour.

- Dossier médical du patient :
  Le dossier médical du patient est hébergé sur une **plateforme externe** (en Belgique ce serait ehealth), c'est donc elle qui est **responsable** du dossier.
  Le **médecin** effectue des **modifications** sur celui-ci après avoir reçu un **patient** en **consultation**. Le médecin tient le patient **informé** et ce dernier peut aussi accéder à son dossier s'il souhaite en connaitre le contenu.
  Il est possible qu'un **confrère** soit **consulté** pour profiter de son expertise.

2.1.2 Périmètre métier et technique

Voir Figure 2 dans les Annexes.

La seconde étape de ce premier atelier est de définir la mission du cabinet médical ainsi que ses valeurs métiers. Au moyen du schéma suivant, nous avons défini ces valeurs métiers ainsi que leur besoin de sécurité et les assets lié à ces valeurs.

- Gestion des RDV : c'est-à-dire la prise, la modification ou l'annulation des RDV. Gestion de l'agenda intervient ici car ils sont liés. Nous considérons le niveau de sécurité nécessaire comme élevé car cette valeur métier permet le bon fonctionnement du cabinet avec les RDV des patients enregistrés.
  Pour son bon fonctionnement, les biens de supports sont : le logiciel de gestion de l'agenda et PC de la secrétaire ainsi que la secrétaire en tant que ressource humaine.

- Informations de contact du patient : Ce sont les coordonnées de contact d'un patient comme son numéro de téléphone, son adresse, … Ceci est noté comme élevé car ce sont des données personnelles et qu'elles permettent de recontacter le patient en cas de suivi. Pour son bon fonctionnement, les biens de supports sont : le logiciel pour gérer le dossier du patient et le PC de la secrétaire ainsi que la secrétaire.

- Suivi médical : le suivi d'un patient au moyen de notes sur une consultation ou d'un enregistrement vocal pour 'plus tard'. Nous considérons cela comme une information car ce sont des informations écrites ou vocales à propos d'un patient. C'est une valeur métier notée basse car il suffit de contacter la partie prenante (le médecin, le patient, le confrère, le service de prise de sang par exemple) pour obtenir les informations qu'il

faut. Pour son bon fonctionnement, les biens de supports sont : le logiciel pour gérer le dossier du patient, le PC du médecin et le médecin lui-même.

- Dossier médical : c'est la consultation et la modification des informations du dossier médical. Idem que pour les informations de contact du patient, ce sont des données personnelles et c'est pourquoi nous l'avons évaluée à 'élevée'. Pour son bon fonctionnement, les biens de supports sont : les identifiants du médecin pour accéder à la plateforme en ligne, le PC du médecin et le médecin.

2.1.3 Évènements redoutés et gravité

Voir Figure 3 dans les Annexes.

Dans cette dernière partie du premier atelier, nous avons listé les évènements redoutés selon les valeurs métiers définies précédemment et nous avons défini un niveau de gravité en nous basant sur l'échelle de l'ANSSI.

- Le service de gestion des rendez-vous :
  Le premier évènement redouté est que l'agenda tombe en panne à la suite d'une attaque, virus, ransomware ou autre. Si un tel évènement survenait, cela entrainerait une impossibilité de travailler car il n'y aurait plus aucune organisation et impossibilité de gérer des RDV. Le niveau de gravité a été défini sur 2 car cet évènement engendrerait surtout un problème d'organisation à cause de l'indisponibilité temporaire de l'agenda mais ne poserait aucun problème quant à la sécurité des patients.

  Le second évènement redouté est la perte des données de rendez-vous à la suite d'une attaque. Cette perte serait une perte totale des informations de rendez-vous et elles ne seraient pas récupérables. Cela engendrerait un gros problème d'organisation car tous les rendez-vous notés seraient perdus, ces rendez-vous pouvant aller sur plusieurs semaines dans le futur. Le niveau de gravité a donc été défini sur 3 car l'indisponibilité des données est irréversible et cette perte engendre une forte dégradation des performances.

- Informations de contact des patients :
  Le premier évènement redouté est la perte des informations de contact des patients par suite d'une attaque. Cela poserait des problèmes pour prendre contact avec le patient. Le niveau de gravité est classé à 2 car les informations sont perdues et pose un problème dans une partie du travail de la secrétaire, ce qui dégrade faiblement les performances mais ne met pas les patients en danger.

  Le second évènement est le vol ou la manipulation de ces données. Cela porterait atteinte à la confidentialité et à l'intégrité des données. Le niveau de gravité a donc été mis à 4 à cause des impacts qu'aurait cet évènement comme une dégradation du travail (impossible de savoir quelles données sont correctes, il faut donc les considérer

comme perdures), cela met aussi les patients en danger si leurs informations sont revendues.

- Le suivi médical :
  L'évènement redouté est la perte des informations sur le suivi des patients par suite d'une attaque. Cela poserait des problèmes pour assurer le suivi d'un patient qui attend des résultats d'analyse par exemple. Le niveau de gravité est classé à 2 car les informations sont perdues et pose un problème dans une partie du travail du médecin, ce qui dégrade faiblement les performances mais ne met pas les patients en danger.

- Le dossier médical :
  Le premier évènement redouté est l'accès à internet qui serait interrompu, ce qui empêcherait notamment d'accéder à la plateforme en ligne hébergeant les dossiers médicaux. Le niveau de gravité est placé à 4 car cela empêcherait le médecin de connaitre les antécédents d'un patient et donc d'établir un diagnostic en toute connaissance de causes ainsi que de le mettre à jour.

  Le second et le troisième évènement redouté sont les identifiants du médecin qui sont compromis (volés et utilisés) et le vol des données du dossier médical pour les revendre. Les deux évènements impliquent une violation de la confidentialité des données médicales et une usurpation de l'identité du médecin. Le niveau de gravité a donc été placé sur 3 pour chacun car les performances du cabinet ne sont pas dégradées mais la sécurité des patients est gravement en danger.

2.2 Atelier 2 : Sources de risques

2.2.1 Sources de risque et objectif visé

Voir Figure 4 dans les Annexes.

La première étape de ce second atelier est la définition des sources de risques ainsi que les objectifs visés par ceux-ci. Ensuite, sur base de leur motivation et de leurs ressources, nous calculons le degré de pertinence de ces risques.

Voici les sources de risques recensées ainsi que leurs objectifs :

- Vengeur, un employé renvoyé et qui souhaite se venger :
  - Interrompre les activités du cabinet, détruire des assets.
  - Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus là-bas
- Amateur :
  - Tester ses compétences par défi, essayer d'obtenir un gain financier par la même occasion
- Crime organisé :
  - Revente d'informations afin d'obtenir un gain financier
- Hacktiviste, personne dont l'idéologie serait complotiste ou anti-médecine occidentale (vaccin, …) :

    - Interrompre les activités du cabinet, détruire des assets.
    - Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus là-bas
- Concurrent :
    - Voler des informations de contact dans le but de voler des patients en les contactant via des prospectus.

Une fois les échelles définies, nous avons pu établir les niveaux de motivation, de ressources, d'activité et de pertinence pour chaque source de risque.

- Vengeur :
    - Fortement motivé
    - Ressources significatives
    - ++++, proche du cabinet médical
    - Plutôt pertinent

- Amateur :
    - Peu motivé
    - Ressources limitées
    - +, n'a rien à voir avec le cabinet
    - Peu pertinent donc

- Crime organisé :
    - Assez motivé
    - Ressources importantes
    - ++, pas proche du cabinet
    - Moyennement pertinent car c'est un cabinet, ce qui représente moins d'inérêt qu'un hôpital mais aussi moins de risques.

- Hacktiviste :
    - Assez motivé
    - Ressources peuvent être significatives
    - ++, pas proche du cabinet
    - Moyennement pertinent

- Concurrent :
    - Assez motivé
    - Ressources significatives
    - ++++, travaille dans le même secteur
    - Plutôt pertinent

2.2.2 Lien entre évènements redoutés et les sources de risque

Voir Figure 5 dans les Annexes.

Sur base des évènements redoutés, nous les avons liés aux sources de risques identifiées afin de mettre en évidence qui pourrait impacter quelle valeur métier :

- Service de gestion de RDV
    - Agenda hors-service suite à une attaque : Vengeur, hacktiviste
    - Perte des données suite à une attaque : Vengeur, hacktiviste

- Informations de contact du patient
    - Perte des données suite à une attaque : Vengeur, hacktiviste
    - Vol ou manipulation des données : Amateur, crime organisé et concurrent

- Suivi médical
    - Perte des données suite à une attaque : Vengeur, hacktiviste

- Dossier médical
    - Connexion à internet interrompue : Vengeur, hacktiviste
    - Identifiants du médecin compromis : Amateur, crime organisé et concurrent
    - Vol pour revente des données : Amateur et crime organisé

2.3 Atelier 3 : Scénarios stratégiques

2.3.1 Niveau de menace

Voir Figure 6 dans les Annexes.

Pour chaque acteur intervenant identifié dans la matrice RACI, nous avons défini leur niveau de menace en identifiant les niveaux de dépendance, de pénétration, de maturité cyber ainsi que la confiance qu'on peut avoir un eux. Au moyen de la formule suivante, le niveau de menace a été déterminé :

$$Niveau\ de\ menace = \frac{\textbf{Taux de pénétration x dépendance}}{\textbf{maturité cyber x confiance}}$$

Les intervenants internes au système :

2. Secrétaire :
    - Dépendance : 2
        - La relation est utile mais pas indispensable car il est possible de trouver d'autre secrétaire
    - Taux de pénétration : 4
        - Elle a accès aux données de contact des patients
    - Maturité : 1
        - Elle n'est probablement pas formée aux risques cyber
    - Confiance : 2
        - Elle est neutre vis-à-vis du cabinet, elle pourrait être tentée de fournir quelques informations en échange d'un gros pot de vin.
    - Menace : 4

3. Médecin :
    - Dépendance : 4

        - Sans le médecin, il est impossible pour le cabinet de fonctionner mis à part la gestion des rendez-vous.
    - Taux de pénétration : 3
        - Il a accès aux données médicales des patients
    - Maturité : 2
        - Il est probablement au courant qu'il faut un peu de sécurité mais sans l'appliquer sérieusement.
    - Confiance : 2
        - Ses intentions sont neutres.
    - Menace : 3

Les intervenants externes au système :

- Patient :
    - Dépendance : 3
        - Si aucun patient ne vient au cabinet, le cabinet ne fonctionne pas.
    - Taux de pénétration : 1
        - Il n'a aucun accès ni connaissance du système.
    - Maturité : 1
        - Il n'intervient pas dans le système, donc il n'est pas impliqué dans sa sécurité cyber.
    - Confiance : 1
        - On ne connait pas ses intentions.
    - Menace : 3

- Confrère :
    - Dépendance : 2
        - Son expertise peut être nécessaire.
    - Taux de pénétration : 1
        - Il n'a aucun accès
    - Maturité : 1
        - Il n'est probablement pas formé aux risques cyber.
    - Confiance : 1
        - On ne connait pas ses intentions.
    - Menace : 2

- Plateforme :
    - Dépendance : 4
        - Sans elle, impossible d'obtenir les dossiers médicaux et donc de travailler correctement.
    - Taux de pénétration : 3
        - Elle possède les dossiers médicaux et est essentielle
    - Maturité : 4
        - Étant donné qu'elle héberge les dossiers médicaux nationaux, elle se doit d'être extrêmement sécurisée.
    - Confiance : 3
        - On connait les intentions et elles sont probablement positives.

- Menace : 1

Dans les Annexes, vous pourrez retrouver une cible représentant les différents niveaux de menaces et d'acceptabilité des menaces à la Figure 7a.

Afin de diminuer les niveaux de menaces, il faut soit augmenter la confiance/maturité soit diminuer la dépendance/pénétration.

2.3.2 Scénarios stratégiques

Voir Figures 8 et 9 dans les Annexes.

Le **1er scénario stratégique** est celui concernant l'employé vengeur et l'hacktiviste qui ont tous les deux pour buts d'interrompre les activités du cabinet et/ou de dénigrer le cabinet auprès des patients pour que ce dernier les perde.

Le vengeur voudra arrêter la prise de rdv par compromission (via une clé USB piégée, phishing) du PC de la secrétaire. Pour cela il passe par la secrétaire et puis par le PC ou bien directement par ce dernier. Ce qui lui permettra d'atteindre les données de gestion des RDV ou de contact des clients.
Ensuite, il a la possibilité de passer par le PC du médecin pour atteindre les données de suivi médical et de les détruire.

Le vengeur comme l'hacktiviste peuvent également tenter de passer par le serveur mail afin d'accéder aux données citées depuis l'intérieur du système.

L'hacktiviste peut, lui, vouloir interrompre la connexion à internet afin d'empêcher le cabinet d'accéder aux dossiers médicaux.

Le **2ème scénario stratégique** concerne l'amateur, le crime organisé et le concurrent qui veulent tous les 3 voler des informations.

Les 3 peuvent passer par le PC de la secrétaire pour obtenir un accès et voler les données des informations de contact des patients. Le crime organisé et le concurrent pourraient oser passer par la secrétaire directement afin d'obtenir les mêmes données.

L'amateur et le crime organisé peuvent décider d'attaquer le PC du médecin ou le serveur mail afin d'obtenir les identifiants de ce dernier et soit les revendre soit les utiliser pour accéder aux données des dossiers médicaux et les revendre. Il est aussi possible qu'une session soit déjà ouverte sur le PC du médecin, ce qui donnerait l'accès aux attaquants sans avoir besoin des identifiants.

2.3.3 Niveau de menace résiduelle

Voir les Figures 7b, 7c et 10 dans les Annexes.

Ces différents scénarios nous ont amené à déjà réfléchir aux mesures qui peuvent être apportées afin de réduire le niveau de menace précédemment calculé :

Partie prenante	Chemins d'attaque	Mesures de sécurité	Menace initiale	Menace résiduelle
Secrétaire	Vengeur qui arrête de la prise de rdv par compromission (via une clé USB piégée, phishing) du pc de la secrétaire	Blocage des ports USB. Formation du personnel aux risques cyber.	4	1
Secrétaire	Le crime organisé et/ou concurrent offrent un pot de vin ou menacent pour accéder aux infos de contact des patients	Avantages extra-légaux. Clause contractuelle de non-divulgation.	4	1
Secrétaire	Pièce jointe piégée par l'envoi de mail frauduleux ou clé USB piégée pour atteindre les données de contact des clients.	Blocage des ports USB. Formation du personnel aux risques cyber.	4	1
Plateforme en ligne	Arrêt de l'activité générale dû à une coupure d'internet volontaire	Avoir une seconde ligne internet (redondance des câbles, boitier 4G).	1	0.75
Médecin	Pièce jointe piégée par l'envoi de mail frauduleux ou clé USB piégée pour obtenir les identifiants du médecin	Installation d'une solution de sécurité (AV). Formation du personnel aux risques cyber.	3	0.89
Médecin	Utilisation des identifiants du médecin ou d'une session ouverte pour voler des données des dossiers médicaux	Forcer le médecin à changer de mdp régulièrement. Double authentification. Monitoring des accès.	3	0.89

2.4 Atelier 4 : Scénarios opérationnels

2.4.1 Scénarios organisationnels

Dans cet atelier, nous allons aborder les différents scénarios organisationnels, soit les différents plans détaillés, utilisés par les acteurs définis plus haut, qui vont décrire comment ces derniers atteindront leurs objectifs à court ou long terme.

Nous avons pour cela créer différents cas possibles, sous forme de schéma, que vous pouvez retrouver dans l'annexe section 1.4.1.

Je vais maintenant vous présenter les différents scénarios et ce en suivant l'ordre dans lequel ils apparaissent dans l'annexe.

Le 1er scénario représente le cas où un « vengeur », par exemple : un ancien employé qui aurait été viré, souhaite la perte de l'ensemble des données « vitales » qui sont en possession de son ancien employeur.

Pour ce faire, deux cas de figure ont été envisagés :

- Le « vengeur » va donc s'introduire dans le système en utilisant le « phishing » afin d'obtenir un contrôle à distance de la machine. Ce qui lui permettra de trouver et supprimer l'ensemble des fichiers qui l'intéressent.
- Le « vengeur » va utiliser une clé USB piratée pour se connecter à distance à la machine et supprimer l'ensemble des fichiers qu'il juge importants pour le cabinet.

Dans les deux cas, le résultat sera une perte totale des informations concernant la gestion des rendez-vous. Ce résultat étant problématique nous avons décidé de le classer à 3 sur notre échelle.

Le 2ème scénario représente le cas où un hacktiviste souhaite interrompre l'activité du cabinet.

Pour ce faire, nous avons imaginé un cas de figure :

- L'hacktiviste serait en mesure de reconnaître et donc de couper les câbles internet. Ce qui engendrerait que le cabinet serait privé pendant un laps de temps plus ou moins grand d'internet. Ce qui aurait comme conséquence l'impossibilité de se connecter à la plateforme en ligne et donc de mettre à jour le dossier de ces derniers.

Pour nous, ce 2ème scénario n'est pas très grave. En effet, rien n'empêche le médecin de prendre des notes manuscrites ou sur son pc, en local, et de les transférer ensuite sur la plateforme.

Le 3ème scénario représente le cas où un hacker amateur, un groupe criminel (= crime organisé), un cabinet concurrent souhaitent voler les informations des clients du cabinet.

Pour ce faire, quatre cas de figure ont été envisagés :

- Ils vont donc s'introduire dans le système en utilisant le « phishing » /pièce jointe malicieuse afin d'obtenir un contrôle à distance de la machine. Ce qui leur permettra de trouver les fichiers qu'ils jugent intéressants et de récupérer l'ensemble des données des clients.
- Ils vont utiliser une clé USB piratée pour se connecter à distance à la machine et récupérer l'ensemble des fichiers clients du cabinet.
- Ils pourraient également menacer l'intégrité de la secrétaire pour récupérer ces différents dossiers.
- Ils pourraient voler l'ordinateur et s'enfuir avec.

Dans les quatre cas, le résultat sera le vol de l'ensemble des informations des client.
Ce résultat est très problématique puisque ces dossiers contiennent des informations confidentielles des clients, telles que l'adresse, le numéro de téléphone, etc.

Le 4ème scénario représente le cas où un hacker amateur et un groupe criminel (= crime organisé) souhaitent voler les identifiants du médecin et ce afin de pouvoir ce connecter sur la plateforme en ligne.

Pour ce faire, deux cas de figure ont été envisagés :

- Ils vont donc s'introduire dans le système en utilisant le « phishing » /pièce jointe malicieuse afin d'obtenir un contrôle à distance de la machine. Ce qui leur permettra d'obtenir les identifiants du médecin.
- Ils pourraient également, grâce à ce contrôle à distance, utiliser un keylogger qui leur permettraient d'enregistrer toutes les frappes de touches du clavier qu'il faudrait ensuite analyser pour trouver le bon mot de passe.

Dans ces deux cas, le résultat pourrait être fortement problématique. En effet, en ayant connaissances des identifiants du médecin ils auraient accès à la plateforme et pourraient donc voler différentes informations, mais également supprimer des fichiers ou encore en modifier. Le plus problématique est qu'il faudrait ce rendre compte que les identifiants du médecin ont été volés et ce n'est pas toujours évident.

Le 5ème scénario représente le cas où un groupe criminel (= crime organisé) souhaitent voler données médicales sur la plateforme en ligne.

Pour ce faire, deux cas de figure ont été envisagés :

- Ils vont donc s'introduire dans le système en utilisant le « phishing » /pièce jointe malicieuse afin d'obtenir un contrôle à distance de la machine. Ce qui leur permettra d'obtenir les identifiants du médecin pour ensuite trouver les fichiers qu'ils jugent intéressants et de récupérer l'ensemble des données médicales des clients.
- Ils vont utiliser une pièce jointe malicieuse pour se connecter à distance à la machine et ensuite soit récupérer directement les identifiants du médecin soit utilisé un keylogger. Une fois ces identifiants obtenus ils pourront se connecter à la plateforme et récupérer l'ensemble des données médicales clients du cabinet. Si le médecin était déjà connecté à la plateforme alors, ils leurs suffit juste de télécharger les différents dossiers qui les intéressent et récupérer les données médicales des clients.

Dans ces différents cas, le résultat pourrait être fortement problématique. En effet, en ayant accès à la plateforme, ils peuvent voler différentes informations, mais également supprimer des fichiers ou encore en modifier. Le plus problématique est qu'il faudrait se rendre compte que des personnes malveillantes « se baladent » sur la plateforme et ce n'est pas toujours évident.

2.5 Atelier 5 : Traitement du risque

Dans cet atelier, nous allons utiliser les scénarios que nous avons créés précédemment pour définir une stratégie de gestion des risques et identifier les risques résiduels.

Nous allons commencer par résumer les risques que nous avons identifiés dans les précédents ateliers et de récupérer leur gravite et probabilité. Si nous reprenons ceux-ci, nous en retrouvons cinq :

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV	
	Gravité : 3	Pr : 3
R2	Hacktiviste qui souhaite interrompre l'activité du cabinet	
	Gravité : 4	Pr : 1
R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients	
	Gravité : 4	Pr : 3
R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin	
	Gravité : 3	Pr : 3
R5	Amateur et crime organisé qui souhaitent voler les informations médicales	
	Gravité : 3	Pr : 3

Grâce à ces risques, nous allons constituer une matrice avec la probabilité pour l'axe x et la gravite pour l'axe y. Cette matrice montrera l'acceptabilité des risques identifiés et les classera dans trois catégories distinctes : acceptable, tolérable et intolérable.

	A	B	C	D	E	F	G	H	I
1	Severity								
2	4	R2		R3				Risk level	Risk acceptability
3	3			R1, R4, R5				Level 1	Acceptable
4	2							Level 2	Tolerable
5	1							Level 3	Unacceptable
6	Likelihood	1	2	3	4				

Nous allons ensuite décider une stratégie de gestion pour chacun de ces risques afin de définir des mesures de traitement.

Il existe quatre manières de traiter un risque :

1. Le maintenir ou l'accepter ; Ce qui veut dire que l'on accepte le risque car son impact ou sa probabilité est négligeable.
2. Le rejeter ; Ce qui veut dire que l'on n'accepte pas ce risque et qu'il est nécessaire de le traiter complètement afin de protéger le bon déroulement de l'entreprise.
3. Le réduire ou le modifier ; Ce qui veut dire qu'on va mettre en place des mesures de traitement de risque afin de réduire la probabilité et la sévérité du risque afin de le rendre négligeable.
4. Le transférer ou le partager ; Ce qui veut dire que l'on va transmettre la responsabilité de ce risque à quelqu'un d'autre. Exemple : souscrire une assurance.

Voici donc les stratégies que nous avons définies pour nos risques :

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV Gravité : 3 Pr : 3	Strategy : Reduce
R2	Hacktiviste qui souhaite interrompre l'activité du cabinet Gravité : 4 Pr : 1	Strategy : Reduce
R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients Gravité : 4 Pr : 3	Strategy : Reject
R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin Gravité : 3 Pr : 3	Strategy : Reject
R5	Amateur et crime organisé qui souhaitent voler les informations médicales Gravité : 3 Pr : 3	Strategy : Reject

Nous avons donc cherché des solutions de traitement pour ces risques et nous sommes arrivés à ce résultat :

Control	Affected risk scenarios	Responsible entity	Implementation difficulties	Cost/complexity
Governance				
Blocage des ports USB	R1	Prestataire IT	Matériel compatible	Peu
Forcer le changement de MDP régulièrement	R4, R5	Prestataire IT		Moyen
Proposer des avantages extra-légaux	R3	Secrétariat social	S'accorder sur les avantages	Moyen
Double authentification	R4, R5	Prestataire IT		Peu
Clause de non divulgation dans les contrats	R3	Secrétariat social		Peu
Prevention				
Mettre d'autres PC à disposition	R1, R2	Prestataire IT		Peu
Cryptage des données	R1, R3	Prestataire IT	Sélectionner le produit de chiffrement	Moyen
Formation du personnel	R1, R2	Prestataire IT		Moyen
Effectuer des simulations pour voir la réaction de la secrétaire face à un pot de vin	R3	Prestataire IT	Coût d'un consultant	Beaucoup
Detection				
IPS/AV/FW	R3	Prestataire IT		Beaucoup
Monitorer les accès	R4, R5	Prestataire IT		Beaucoup
Recovery				
Backup	R1, R2	Prestataire IT	Coût du processus	Beaucoup
Redondance de la ligne internet	R2	Prestataire IT		Moyen

Ces différentes solutions permettront de diminuer la probabilité et la sévérité de nos risques.

Nous pouvons donc recalculer celles-ci pour chacun de nos risques :

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV	
	Gravité : 1	Pr : 1

Pour notre premier risque, le fait d'effectuer un blocage des ports USB, d'effectuer un cryptage du disque dur de la secrétaire, de former celle-ci aux phishings et aux risques informatiques permet de diminuer la probabilité de notre risque à 1.

Le fait de prévoir une solution de backup et une machine de rechange nous permet d'également diminuer l'impact à 1.

R2	Hacktiviste qui souhaite interrompre l'activité du cabinet						
	Gravité : 1	Pr : 1					

Pour notre deuxième risque, le fait de former la secrétaire aux bonnes pratiques informatique (ne pas insérer une clé USB inconnue dans son pc, ne pas cliquer / répondre à un mail imprévu …) permettent de diminuer la probabilité de notre risque à 1.

Le fait de prévoir une solution de backup, un autre ordinateur et une redondance de la ligne internet du cabinet nous permet d'également diminuer la gravite de notre risque à 1.

R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients						
	Gravité : 2	Pr : 3					

Concernant notre troisième risque, nous avons trouvé comme solution d'offrir des avantages extra-légaux à la secrétaire afin d'augmenter sa fidélité ainsi que d'inclure une clause de non-divulgation dans son contrat. Une simulation de pot de vin / phishing effectuée par un consultant permettrait d'évaluer la réaction de la secrétaire à ce type de menace.

Nous avons également imaginé la mise en place de solutions de sécurité tel qu'une solution antivirus, un firewall ou un IPS afin de détecter et de bloquer un piratage de son ordinateur. Cependant, malgré toutes ces solutions, nous avons estimé que la probabilité ne diminuerait que à 3 car aucunes de ces solutions n'exclue complément le risque.

Pour la gravité de ce risque, un cryptage du disque dur de la secrétaire permettrait d'empêcher celui-ci d'être voler ce qui diminuerait la gravité du risque à 2.

R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin						
	Gravité : 3	Pr : 1					
R5	Amateur et crime organisé qui souhaitent voler les informations médicales						
	Gravité : 3	Pr : 1					

Les deux derniers risques sont assez similaires car les chemins d'attaque sont similaires, seul l'objectif est différent.

Pour ceux-ci, le fait d'implémenter une politique de changement de mot de passe régulière, de mettre en place la double authentification et de monitorer les accès du médecin diminue la probabilité de ces risques à 1. La gravite reste cependant inchangée.

Grâce à ces nouvelles valeurs, il nous a été possible d'effectuer une nouvelle matrice et de constater que la majorité de nos risques sont devenus acceptables. Seul le risque trois reste tolérable car celui-ci concerne des données personnelles.

Severity							
4						Risk level	Risk acceptability
3	R4, R5					Level 1	Acceptable
2			R3			Level 2	Tolerable
1	R1, R2					Level 3	Unacceptable
Likelihood	1	2	3	4			

3 Conclusion

Pour conclure, la gestion des risques est primordiale pour tous cabinets médicaux. En effet, en plus d'être confronté à des risques de types « médicales », ils sont aujourd'hui confrontés à des risques de types informatiques (nous ne nous sommes pas intéressés aux risques médicaux dans ce cas-ci).

Il est donc nécessaire de mettre en place une stratégie de gestion de risques adapté à cet environnement et à ses activités. Ce qui comprend la formation du personnel, augmenter de manière drastique la sécurité déjà présente, …

En mettant en place, ces différentes mesures, le cabinet médical est alors sûr de réduire les risques pour son personnel, son infrastructure ainsi que pour ses patients.