# Rapport théorique

***Aspects du document qui peuvent s'appliquer dans le cadre de l'intégration dans la structure dans laquelle on travaille et sur le projet conduisant au développement de notre application Web :***

Aujourd'hui, sécuriser son projet est devenu primordial du fait des nombreuses attaques et conséquences que cela peut entraîner. Il faut évidemment distinguer la sécurité du système d'information où se trouvera le projet, et la sécurité du projet lui même.
Généralement, pour sécuriser correctement un projet, il faut respecter plusieurs points importants :

- Tout d'abord il faut prendre en compte la sécurité à toutes les étapes du projet. En effet, une grande erreur à ne pas faire est de ne prendre en compte la sécurité qu'à la fin du développement. Cela pourrait entraîner :
• Coûts (parfois importants) supplémentaires ;
• Besoin de recréer certains éléments et de faire des modifications conséquentes ;
• Besoin de rajouter certains éléments ;
• Retard dans la durée du projet

- Ensuite, il faut analyser les risque pour :
• Identifier les biens à protéger
• Analyser le danger pour mieux évaluer le risque
• Établir une hiérarchisation des risques : fréquence vs gravité
• Établir un seuil d'acceptabilité pour chacun de ces risques
• Seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité.
• Identifier des mesures de sécurité.

- Après l'analyse des risques, afin de mettre en place des mesures de sécurité, il faut respecter le principe de la défense en profondeur, qui a pour objectifs de prévenir, bloquer, limiter, détecter, alerter, réagir, réparer. Cette analyse recommande :
• d'avoir plusieurs lignes de défenses indépendantes
• que chaque ligne constitue une barrière autonome contre les attaques
• que derrière chaque ligne de défense passée, on arrive à une plus forte

De nombreuses normes permettent la mise en place de la sécurité au sein d'une organisation, telles que :
- La norme ISO 27001 permet à une organisation de mettre en œuvre et d'améliorer le système de sécurité. Après quoi l'entreprise reçoit une certification comme quoi elle respecte bien cette norme.
- La norme ISO 27002 qui résume les bonnes pratiques et les bons comportements à avoir.
– La norme ISO 27005 qui définit clairement comment doit se comporter le système de gestion des risques et de la sécurité

Mais pourquoi parfois, les entreprises ne prennent pas en compte la sécurité dans un projet ? Pourtant, des nombreux risques très dommageables sont possibles ! Plusieurs facteurs permettent de répondre à cette question :

- Manque de conscience des dirigeants, qui ne pensent pas nécessaire d'ultra sécuriser le réseau.
- Personnel issue d'un secteur où la sécurité n'est pas mise en avant, donc ne prend pas ça à cœur
- Coût qui dissuade les dirigeants
- Mauvaise compréhension des enjeux : certaines entreprises ne savent pas ce que peut entraîner une mauvaise sécurité : fuite d'informations, mauvaise image publicitaire etc.
- La sécurité ne dépend pas que des dirigeants, mais aussi des employés. Tout le monde doit donc être motivé, responsabilisé et impliqué ! Sans quoi rien ne sert d'investir dans la sécurité, il y aura toujours des failles !
- Difficulté de faire confiance aux prestataires extérieurs ou au matériel nécessaire à la sécurisation.
- Peur d'avoir une mauvaise productivité si on est restreint par des règles et contrainte informatiques.

En conclusion, il convient à l'entreprise d'être conscient des enjeux de la sécurité et de mettre en place un système respectant plusieurs points important. Pour ce faire, elle se doit de respecter les normes principales de sécurité, qui permettront d'éviter d'éventuelles attaques.

***Différence de comportement entre une « route protégée » et un contrôleur modifiant le contenu :***

Une route protégée se définit par Auth::routes(), qui permet de générer toutes les routes requises pour l'authentification de l'utilisateur. Ainsi, grâce à cela, l'éventuel cyberattaquant ne pourra plus retrouver la bonne route qui permet de sécuriser la connexion d'un utilisateur, car les méthodes se trouvent directement à l'intérieur de Laravel.

Le contrôleur PasswordController permet de modifier un mot de passe en cas d'oubli par l'utilisateur. Lui aussi utilise des méthodes qui se trouvent dans le framework lui même, et permet donc une bonne sécurisation.