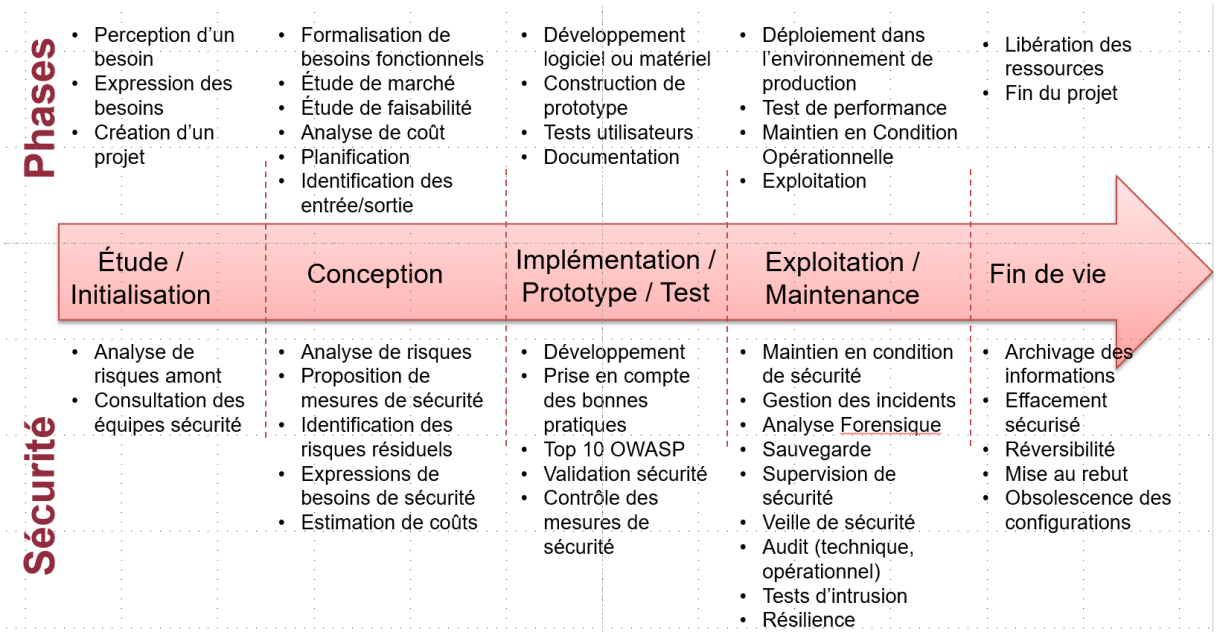
Module 2 – CyberEdu A7 : Intégrer la sécurité dans le projet

La sécurité des projets représente un enjeu très important pour les entreprises qui les développent. En effet, chaque projet doit être sécurisé en appliquant la réglementation en cours et l'organisation cohérente de celle-ci dans le projet dans le but d'avoir une sécurité forte. Il faut d'abord faire la différence entre la sécurité du système d'information en lui-même et la sécurité du projet en lui-même, cette sécurité est présente à chaque étape du projet. Il existe différents documents qui peuvent nous aider lors de chaque phase du projet et qui doivent être rapportés dans le cahier des charges du projet. On distingue les nécessitées suivantes :

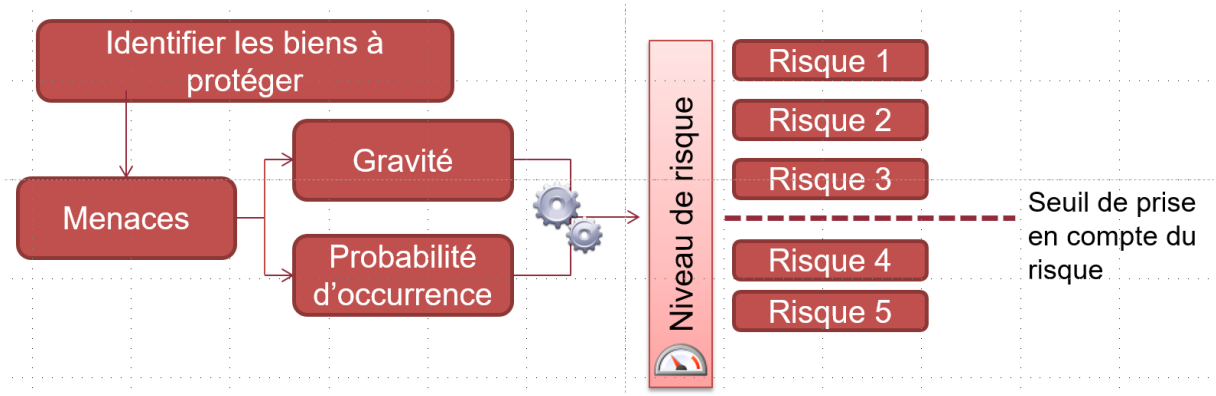


Il en faut pas que se concentrer sur la sécurité du projet mais aussi sur les ressources que celui-ci nécessite comme par exemple des bases de données, des composantes logicielles obsolètes ou encore des politiques de mot de passes non respectées. Si des problèmes sont rencontrés cela peut engendrer différents problèmes comme le retrait de l'application pour un temps inconnu afin de trouver les bugs, donc implicitement des coûts supplémentaires ou des modifications d'infrastructures.

Il existe néanmoins des moyens d'analyse et de traitement des risques possibles. Il est nécessaire de l'effectuer en amont et de pair avec le projet, on retrouve par exemple :

- Identifier les biens à protéger
- Analyse de la fréquence et de la gravité du danger pour évaluer la criticité du risque
- Etablir une hiérarchisation du risque : fréquence opposée à gravité
- …

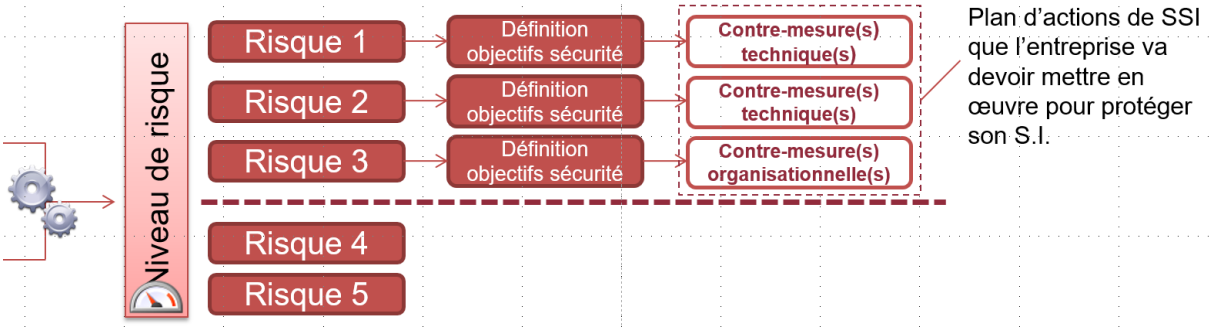
Une analyse de risque se passe de la façon suivante :



Il existe 2 types de risques et donc 2 types de traitements différents :

- Si le risque est supérieur au seuil de prise en compte alors :
  - Il faut définir les objectifs de sécurité
  - Définir les mesures techniques et organisationnelles qui vont permettre de les atteindre
- Si le risque est inférieur au seuil de prise en compte alors:
  - On peut le considérer comme un risque résiduel (dont le traitement coûtera trop cher par rapport à la gravité du risque)

On approche le risque de la façon suivante :

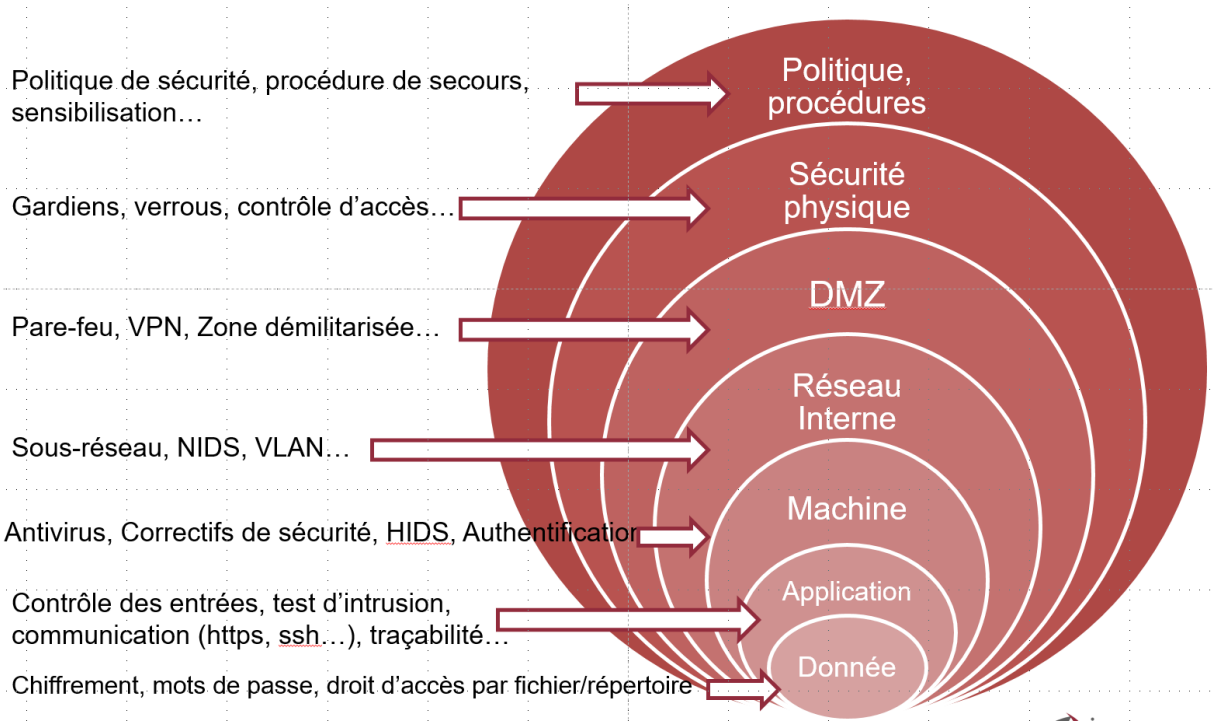


L'analyse de ce risque peut être complexe et doit donc être effectuée avec rigueur et minutie, il faut trouver le bon niveau d'abstraction. Il existe de nombreuses méthodes d'analyse du risque compatibles avec l'article qui les contiens, l'article ISO 27005. On peut citer les méthodes EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), MEHARI (MEthode Harmonisée d'Analyse du Risque) ou encore OCTAVE (Operationaly Critical Threat, Asset, and Vulnerability Evaluation).

La mise en place d'une sécurité est un défi asymétrique car il mêle "attaque" et "défense" :

- L'attaque peut réussir par l'exploitation d'une seule et unique vulnérabilité
- La défense doit prendre en compte l'ensemble du système

Le principe de "défense en profondeur" est recommandé, il permet par l'instauration de plusieurs couches, chacune étant une barrière autonome contre les attaques, chacune comportant un niveau de sécurité différent se renforçant au fur et à mesure que l'on s'approche du centre. Il peut être schématisé ainsi :



Nous avons appris à utiliser le cryptage MD5 ou Message Digest 5 qui est une fonction de hachage cryptographique permettant d'obtenir l'empreinte numérique d'un fichier. Nous l'avons utilisé avec le langage pHp. Cette fonction nous a permis de crypter des mots de passes client dans une base de données afin que ceux-ci ne soient pas écrit en clair dans la base de donnée ce qui serai fâcheux si celle-ci venait à être piratée. Voici le résultat obtenu :

+ Options

	id_user	login	pass	nom	prenom	privilege
Éditer Copier Supprimer	1	user1	24c9e15e52afc47c225b757e7bee1f9d	BERTIN	Jérome	admin
Éditer Copier Supprimer	10	test	721a9b52bfceacc503c056e3b9b93cfa	Meslin	Thibaut	admin
Éditer Copier Supprimer	9	meslin	721a9b52bfceacc503c056e3b9b93cfa	MESLIN	Thibaut	user

```php
if (isset($_POST['login'])){ // execution uniquement apres envoi du formulaire (test si la variable POST existe)
  // mise en variable du nom d'utilisateur
  $login = $_POST['login'];
  // mise en variable du mot de passe chiffré à l'aide de md5
  $mdp = md5($_POST['pass']);
  // requête sur la table utilisateurs (on récupère les infos de la personne)
  $sql = "SELECT pass FROM utilisateurs WHERE login = '$login'";
  // Exécution de la requête
  $exec = mysqli_query($lienBd,$sql);

  if (mysqli_num_rows($exec) > 0) { // On test s'il y a un utilisateur correspondant

    // récupération des infos

    // déclaration des variables de session
    $login = $_SESSION['login'];
    $mdp = $_SESSION['pass'];

    $connexion=true;
    header("Location:admin.php"); // redirection si OK
  }
  else {
    $connexion=false;
  }
}

?>
```