**Sécurité applicative**

**Contexte**

« La sécurité des applications est un processus effectué pour appliquer des contrôles et des mesures aux applications d’une organisation afin de gérer le risque de leur utilisation ».

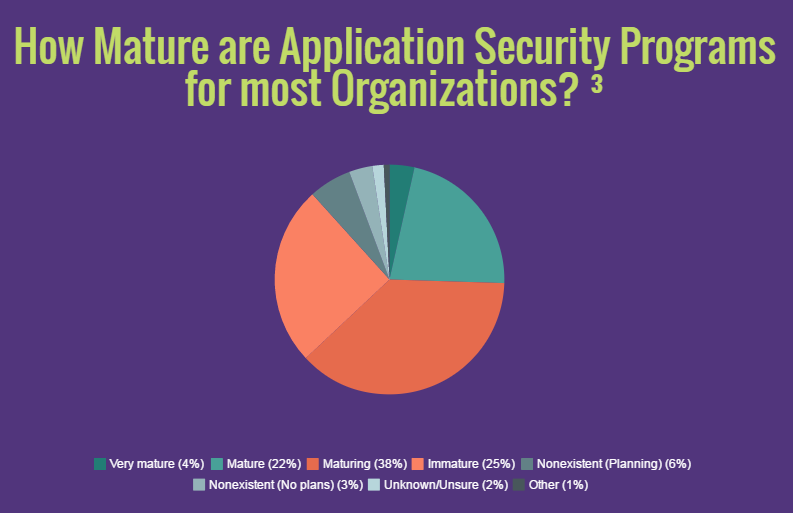
« Les contrôles et les mesures peuvent être appliquées à l'application elle-même (ses processus, les composants, les logiciels et résultats), à ses données (données de configuration, les données de l'utilisateur, les données de l'organisation), et à toutes les technologies, les processus et acteurs impliqués dans le cycle de vie de l'application ».

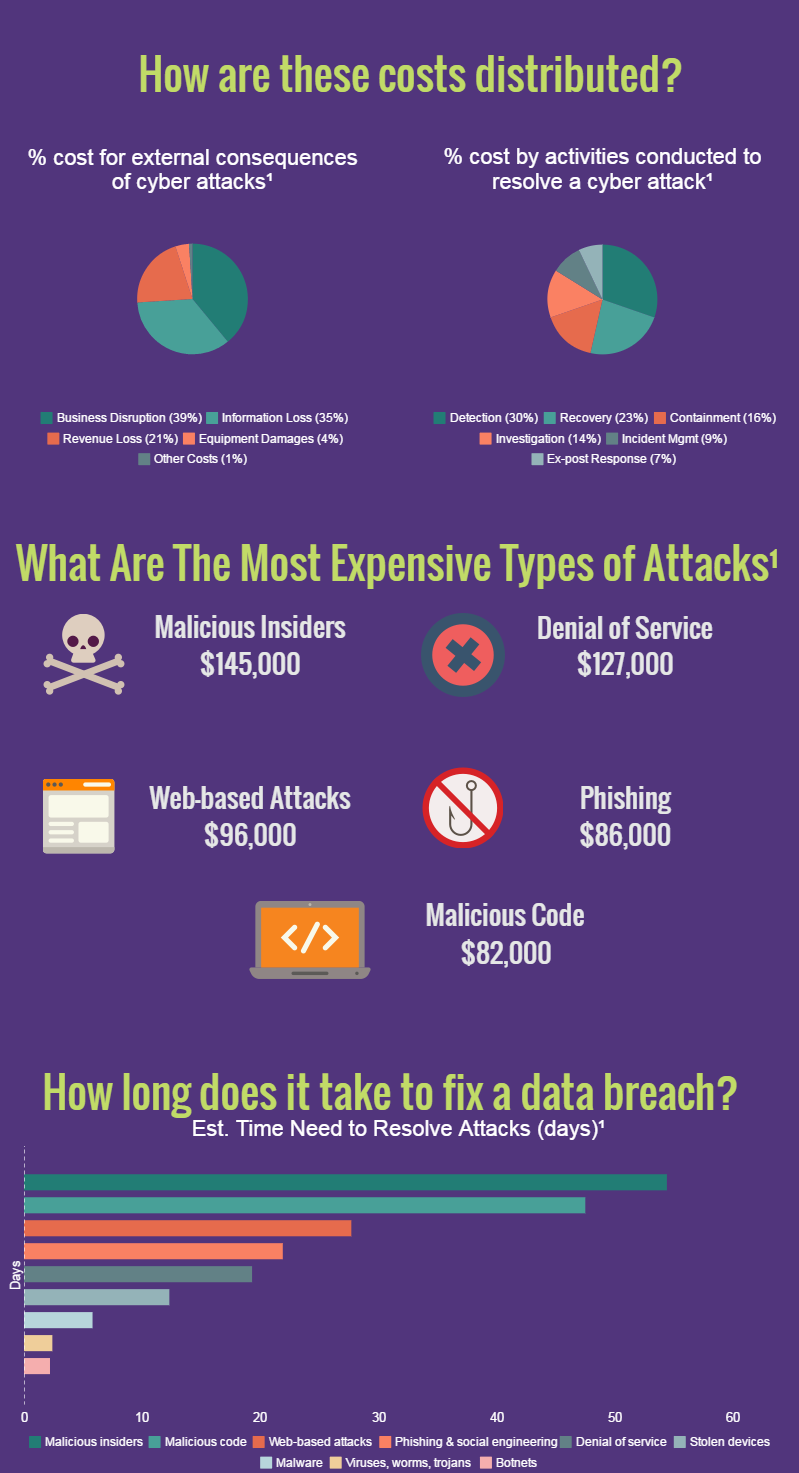
*Source : ISO 27034*

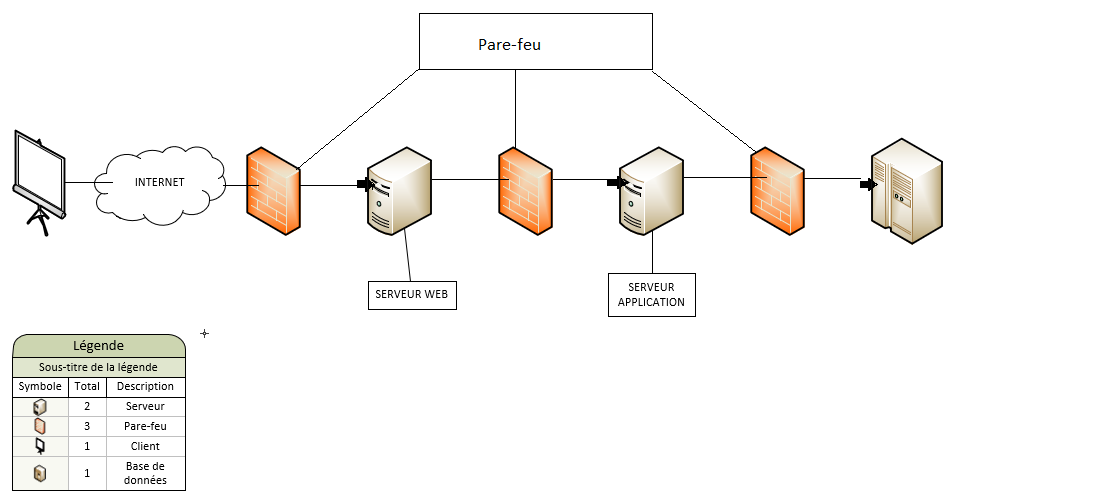
Selon quelques statistiques :

* 84% des attaques ciblent la couche applicative*. Source : Checkmarx 2015*.
* 75% des vulnérabilités se trouvent dans la couche applicative. *Source : Checkmarx 2015.*

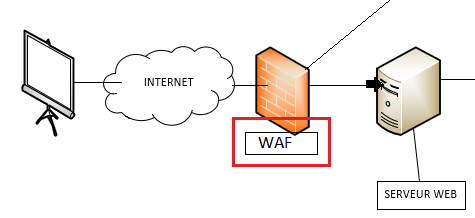
Dans le contexte de l’entreprise MADERA, la pérennité de l’entreprise se joue également sur la sécurité de l’application WEB que nous allons livrer.   
Le SI tout entier est donc un risque très important de fuite de données.

(Une fuite de données coûte à une entreprise en moyenne 3,92 millions de dollars, soit 150 dollars par document perdu. Selon une étude commanditée par IBM Security.)  
*source : Checkmarx website*

  
 *source : Checkmarx website*

**Schéma global de la sécurisation d’une application.**

L’ajout de Firewalls permet de prévenir les intrusions et de contrôler les accès. *Le Firewall surveille le périmètre. La porte d’accès est identifiée. On peut bloquer une liste de requêtes ou de personnes. (Blacklist).*

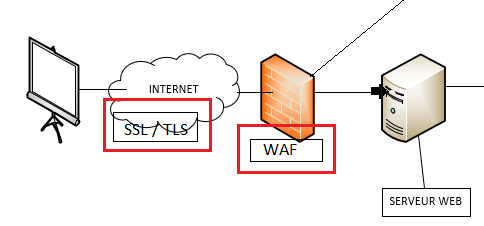
**

Au firewall classique devant le serveur WEB nous pouvons ajouter un Web Application Firewall (WAF)

*Le WAF surveille le comportement. Un système de liste blanche décrit les requêtes normales acceptées. Le reste est décrit comme neutre. Le WAF analyse les réponses. Une suite d’erreur, une quantité anormale de données ou un enchainement anormal d’actions entraine un ajout de la requête en liste noire.*

*Le WAF permet donc de protéger l’application des attaques les plus fréquentes de manière totalement automatisée. Ces attaques sont répertoriées dans le TOP10 Owasp (Open Web Application Security Project).  
Les deux attaques les plus fréquentes sont les SQLI (Injection de commande SQL) et les XSS (référentiel à des scripts externes).*

De plus, il apparait désormais indispensable de chiffrer en SSL (Secure Sockets Layer) voire TLS (Transport Layer Security). Le SSL, permet de se connecter de manière sécurisée à l’application depuis un navigateur.



Crypter les données sensibles comme les mots de passes dans la base de données permet de limiter les risques d’usurpation.

Enfin quelques bonnes pratiques participant à la sécurité d’un SI :

* Limiter les champs libres et contrôler le contenu des insertions en base
* Sensibiliser les utilisateurs
* Gérer les profils utilisateurs
* Gérer le niveau de sécurité/ complexité des mots de passe
* Mettre en place un plan de crise en cas de panne accidentelle ou malveillante