# Gouvernance de la sécurité : Comment garantir la sécurité de l'information dans le contexte d'une PME basée sur un service Web ?

**Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES**

par :

**Flavien GAILLARD**

Conseiller au travail de Bachelor :

**Rolf HAURI (Chargé d'enseignement HES, Directeur du CCSIE, Directeur du MBA MSSI)**

Carouge, le 11 juin 2013

Haute École de Gestion de Genève (HEG-GE)
Filière IG

# Déclaration

Ce travail de diplôme est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre « Bachelor of science HES-SO en Informatique de gestion ». L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de diplôme, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de diplôme, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 11 juin 2013

Flavien GAILLARD

# Remerciements

Pour commencer je tiens à remercier M. Rolf Hauri pour ses conseils et son adaptation concernant mes disponibilités tout au long de la réalisation de mon travail de diplôme.

Je remercie mon très bon ami M. Nicolas Hürzeler qui m'a soutenu tout au long de mon travail.

Et pour terminer merci à mère Mme  Brigitte Gaillard pour la relecture et les corrections.

# Résumé

Ce travail de mémoire a pour but de « comment garantir la sécurité de l'information dans le contexte d'une PME basée sur un service web ». Pour ce faire, diverses menaces concernant les services web ont été identifiées puis classées pour pouvoir définir des mesures palliatives. Ces mesures sont reprises dans un livre blanc qui donne des recommandations pour palier à ces menaces si le service web n'est pas encore protégé contre celles-ci.

J'ai effectué principalement mes recherches en ligne. En procédant ainsi, l'accès aux informations les plus récentes et pertinentes était garanti.

Pour commencer j'ai identifié une liste de menaces dans le cas de la sécurité de l'information d'un service web.

Par la suite l'origine et la dimension de chacune des menaces sont identifiées pour pouvoir définir des mesures contres celle-ci.

Pour compléter cette analyse un livre blanc a été réalisé dans le but de pouvoir évaluer la sécurité de différents services web. A partir de celui-ci, la PME en question peut évaluer son niveau de sécurité face aux menaces décrites. Une fois cette évaluation effectuée, l'entreprise peut prendre les mesures nécessaires pour garantir la sécurité de l'information de son service web.

# Table des matières

## Contenu

# Liste des Tableaux

# Liste des Figures

# Introduction

## 1. Présentation

### *1.1 Choix du sujet*

Depuis les dernières années, de plus en plus de commerces fleurissent sur la toile. Que ce soit pour l'achat de produits, de prestations ou de services, le nombre de ces sites augmente de jour en jour.

Du fait du nombre grandissant de ceux-ci, ils deviennent de plus en plus une cible pour des attaques et les clients eux deviennent de plus en plus exigeants.

J'ai donc choisi de réaliser mon travail sur le thème de la sécurité de l'information d'un service web.

Pour avoir un exemple concret et de pouvoir contrôler mon travail, j'ai la chance de pouvoir l'appliquer à l'entreprise SoSport qui a son business en ligne.

En ayant choisi le thème de la sécurité de l'information, il est donc logique que je me sois tourné vers M. Rolf Hauri, qui est un enseignant spécialisé dans ce domaine.

### *1.2 Présentation de SoSport*

SoSport est une plate-forme web qui permet de gérer des équipes de sport. Depuis ce site, il est possible de centraliser toutes les informations utiles, comme les horaires des matchs et d'entraînements, les statistiques etc. C'est un puissant outil de communication qui permet de garder le contact avec son équipe et d'éviter des dizaines de coups de téléphone, par exemple en cas d'annulation d'un entraînement. Cela permet aussi d'avoir des interactions entre les joueurs, les parents, les entraîneurs et même les supporters.

Le site dispose d'un système d'abonnement mensuel pour les clients réguliers.

Du fait que SoSport soit uniquement accessible en ligne, ce travail permet de pouvoir signaler à l'entreprise à quoi elle doit faire attention et ainsi pouvoir pointer les mesures qui ne sont pas encore (ou en partie) effectives.

# 2. Liste des menaces

## *2.1 Etablissement de la liste*

Pour établir la liste des menaces j'ai procédé de différentes manières. J'ai, dans un premier temps, établi des recherches sur le web. Une de mes principales sources d'information a été le site (http://www.authsecu.com/e-commerce-menaces-protections/e-commerce-menaces-protections.php) qui parle des menaces et des protections de l'E-Commerce. Je me suis également appuyé sur les documents du cours « Sécurité » dispensé par M. Hauri. Pour compléter ma liste, j'ai également pointé les éléments importants des notes prises durant la conférence du CLUSIF qui avait le thème « Un code au-dessus de tout soupçon ».

Etant donné qu'il existe un très grand nombre de menaces encourues par une PME qui a son business en ligne, j'ai établi une sélection de menaces. A partir d'une liste plus conséquente, j'ai sélectionné une partie de celles-ci pour avoir au minimum une menace  par dimension et origine des menaces (D,I,C,N & A,P,M – Voir ci-dessous) . J'ai également retiré ou regroupé les menaces qui étaient semblables ou très proches.

## 2.2 Dimension des menaces

Les menaces concernent les différentes dimensions de la sécurité.

Selon la norme ISO 27000[1] les dimensions sont définies en quatre catégories :

**Disponibilité**

*Propriété d'être accessible et utilisable à la demande par une entité autorisée*

**Intégrité**

*Propriété de protection de l'exactitude et de l'exhaustivité des actifs*

**Confidentialité**

*Propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés*

**Non-répudiation**

*Capacité à prouver l'occurrence d'un événement ou d'une action donnés et les entités qui en sont à l'origine, de manière à prouver l'occurrence ou la non-occurrence de l'événement ou de l'action et l'implication des entités dans l'événement*

## 2.3 Origine des menaces

**Panne - Accident**

Arrêt non prévu du système.

**Erreur**

Problème de conception.

**Malveillance**

Attaque du système dans le but de nuire à son bon fonctionnement.

[1] ORGANISATION INTERNATIONALE DE NORMALISATION. Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire. Genève : ISO, 2009. 57 p. Norme internationale ISO/CEI 27000 : 2009

## 2.4 Tableau des menaces

Chaque menace est identifiée par ça (ou ses dimensions) ainsi que l'origine de la menace dans le tableau ci-dessous :

| N° | Menace | Origine | Dimension |
|---|---|---|---|
| 1 | L'écoute des communications | M | I – C |
| 2 | La substitution de données | M | I – C |
| 3 | Utilisation des bugs des applications | E – M | D – I – C |
| 4 | Déni de service et DDoS | M | D – I – C |
| 5 | Attaques sur la base de données | M | D – I – C |
| 6 | Dévoiler des informations à un concurrent | E | C |
| 7 | Copier-coller malheureux | E | D – I – C |
| 8 | l'ingénierie sociale | M | C |
| 9 | Input des clients risqués (image, fichier pdf) | E – M | D – I – C |
| 10 | Client qui nie avoir prolongé son abonnement au service | E | N |
| 11 | Des données disparaissent suite à une fausse manipulation du client | E | N |
| 12 | Service inaccessible | A M | D |
| 13 | Accès physique aux serveurs | M | D – I – C |

*Origine : Panne - Accident* ***(A)*** *– Erreur* ***(E)*** *- Malveillance* ***(M)***
Dimension : *Disponibilité* ***(D)*** *- Intégrité* ***(I)*** *- Confidentialité* ***(C)*** *- Non-répudiation* ***(N)***

## *2.5 Description des menaces*

Dans cette partie, je vais décrire les différentes menaces que j'ai identifiées dans la première partie de mon travail. Pour chacun de ses risques, je répondrai également à la question « Comment se protéger » dans le chapitre suivant de ce travail.

### 2.5.1 L'écoute des communications

Ce type d'attaque est également appelé « Ecoute passive » ou « rejeu ». Dans ce cas, on parle d'interception de l'information. La plupart du temps, le but est d'obtenir un mot de passe pour accéder à des informations privées. Cela peut être les informations d'une communication entre le client et le fournisseur de service, ou alors à l'une de ses extrémités.

### 2.5.2 La substitution ou manipulation de données

Ce type d'attaque a pour but d'attaquer les données d'un service web. Dans le cas d'un business web, je vais parler de la substitution dans le cas d'une transaction bancaire. En effet, si un client souhaite prolonger son abonnement, il doit réaliser une opération de paiement en ligne. Suivant comment le code est réalisé, le montant de la transaction est passé dans une requête « http post ». Le hacker peut accéder à celle-ci et ainsi en modifier le montant et la destination.

### 2.5.3 Utilisation des bugs des applications

Les hackers utilisent les bugs de l'application pour s'y introduire, dans le but d'y récolter des informations sensibles et d'y placer du code (ou un logiciel) malveillant. Dans le cas d'un service web, le hacker pourrait utiliser une faille pour intercepter les transactions bancaires par exemple.

### 2.5.4 Déni de service et DDoS

Ce type d'attaque a pour but de de rendre indisponible le service web. Donc le rendre indisponible à l'utilisateur ainsi qu'au propriétaire.
Les hackers utilisent ces attaques pour différentes raisons [2]:

- l'inondation d'un réseau afin d'empêcher son fonctionnement
- La perturbation des connexions entre deux machines
- l'obstruction d'accès à un service à une personne en particulier.

Les attaques de ce type actuellement utilisées sont les attaques en déni de service distribué (DDoS). Grâce à des failles connues, les hackers obtiennent les droits administrateurs sur des machines de privé autour du monde. Par la suite, un logiciel malveillant est installé sur ces machines et il est utilisé pour réaliser des attaques sur la cible finale[3].

La plupart du temps ces attaques n'ont pas pour but de récupérer ou d'altérer des données. Le but est de nuire à la société. Il s'agit de quelque chose de très grave dans le fonctionnement d'un service web. En effet, le site n'est plus accessible, les clients qui ont payé pour un abonnement sont mécontents et d'une certaine manière, ils doivent être dédommagés.

[2] WIKIPEDIA - Attaque par déni de service (http://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service) consulté le 12.05.2013

[3] CERTA - Le déni de service distribué (http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001) consulté le 13.05.2013

### 2.5.5 Attaques sur la base de données

Le plus souvent en ligne, le type de base de données utilisé est le SQL. Je vais donc décrire cette menace en me basant sur ce langage de base de données. On parle d'injection de commande SQL qui est un type d'attaque basé sur des bases de données relationnelles.

La faille est souvent due au fait que le concepteur ne fait aucun test sur les paramètres – variables passées dans les requêtes SQL. Ainsi la personne malintentionnée peut accéder à toutes les informations de la base. De plus, il est possible de modifier le contenu ou de le supprimer.

Un exemple simple pour présenter la faille :

Prenons par exemple une requête qui a comme paramètre un nom d'utilisateur.

```
SELECT * FROM users WHERE nom="$nom";
```

En « jouant » sur la variable $nom, il est possible d'allonger la requête et d'utiliser des opérateurs de comparaison. On donne donc à la variable nom la valeur « toto" OR 1=1 »
Notre requête finale se présente donc de cette manière :

```
SELECT * FROM users WHERE nom="toto" OR 1=1;
```

Avec cette requête on peut se rendre compte que l'on aura accès à toutes les informations de la table utilisateur grâce à l'opérateur OR et la comparaison toujours vraie de 1=1.

Pour les services web qui utilisent *Microsoft SQL Server* il existe une faille sur les procédures stockées. En effet, ces procédures permettent de lancer des commandes d'administration. Ainsi un utilisateur malintentionné pourrait exécuter des commandes système pour s'introduire dans la base de données.

### 2.5.6 Dévoiler des informations à un concurrent

Ce type de menace n'est pas une menace technique comme toutes celles qui précèdent. En effet, dévoiler une information à un concurrent dans le domaine informatique peut très vite porter à conséquence.

Selon une étude[4] de lamelee.com

*En général, dans les entreprises :*

- ***5%** de l'information est stratégique : toute information permettant de mettre à nu la valeur ajoutée de l'entreprise ou divulguant ses avantages compétitifs.*
- ***15 %** de l'information est sensible : ensemble des données qui, associées et mises en cohérence, peuvent révéler une partie de l'information stratégique.*
- ***80%** de l'information est divulgué (ouverte) : ensemble des données diffusables à l'extérieur de l'entreprise sans pour autant lui être préjudiciable.*

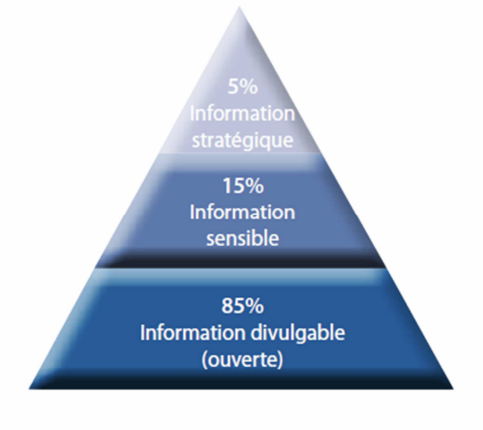


Figure 1

On peut donc constater que la plupart des informations d'une entreprise sont de toute manière diffusées à l'extérieur. Mais la partie la plus critique est l'information stratégique. Il est tout à fait imaginable de se tromper de destinataire lors de l'envoi d'un mail avec pièce-jointe par exemple. Suivant le document, les conséquences peuvent être très graves pour la bonne marche de l'entreprise.

Dans le domaine des services web, il faut également faire attention aux informations divulguées. En effet, il est dangereux d'annoncer une nouvelle fonctionnalité sur les réseaux sociaux, ou autre moyen de communication, si celle-ci n'es pas finalisée. Les concurrents directs consultent ces informations et ils pourraient très bien développer la nouvelle fonctionnalité et la publier avant son concurrent.

[4] LAMELEE.COM - http://www.lamelee.com/les-ressources/securite-de-linformation/securite-des-systemes-dinformation/view.html - PAGE 8 - Consulté le 11.05.2012

### 2.5.7 Copier-coller malheureux

J'ai entendu parler de ce type de menaces pour tous service web lors de la conférence « Un code au-dessus de tout soupçon » organisée par le CLUSIS.

De nos jours, de plus en plus de code est réutilisé pour éviter de passer des heures à coder quelque chose qui existe déjà. Certes cette méthode permet de gagner du temps et de l'argent, mais elle n'est pas sans risque.

Premièrement, si un bout de code est récupéré et implanté dans le programme vous n'êtes pas le seul à l'avoir utilisé. Si l'on imagine que ce code contient des failles, le service web devient donc menacé par les virus qui exploitent déjà ces failles.

Le copier-coller malheureux peut aussi entraîner des ralentissements inutiles de l'application. Il peut arriver qu'une grande partie du code ne soit pas utilisée.

### 2.5.8 L'ingénierie sociale

Les mails sont un important type de communication pour une entreprise qui a son business basé sur un service web. En effet, il est important d'avoir un service après-vente réactif et de pouvoir communiquer les dernières nouveautés aux abonnés du site pour montrer que le service est en constante évolution.

Dans certains cas l'envoi de mail peut nuire au bon fonctionnement du service mail et également donner une mauvaise image de l'entreprise.

En effet, si l'on prend le cas d'un hacker qui prend le contrôle de la boite mail principale.

Il peut envoyer des milliers de mail de spam depuis le compte mail aux abonnés du service. Ainsi, il pourra utiliser la confiance que les utilisateurs ont envers les mails en provenance du site.

On peut également imaginer que le hacker demande des informations bancaires via les mails en redirigeant les abonnés vers un site web de sa création qui a comme unique but la récupération des informations privées des utilisateurs. On appelle ceci l'ingénierie sociale.

On peut également parler du cas où, c'est le code du site en lui-même qui est modifié. Ainsi l'utilisateur procède de manière habituelle au paiement de son abonnement, mais il ne sait pas qu'en fait il est en train d'entrer ses informations bancaires sur un clone de la page.

Dans ces deux cas la mesure efficace est une mesure humaine et préventive.

### 2.5.9 Input des clients risqués (image, fichier pdf)

Ce type de menace survient du moment qu'un service d'upload est proposé à l'utilisateur. Par exemple pour changer sa photo de profil ou alors compléter son profil avec des documents PDF par exemple.

Le but de cette faille est d'uploader un fichier avec une extension non autorisée. (Par exemple un code php) pour pouvoir accéder au serveur cible.

Il existe deux méthodes connues pour l'exploitation de ces failles :

La première méthode s'appelle le « Bypass mime vérification ». Il s'agit d'une méthode qui fonctionne directement depuis Firefox qui consiste à changer la valeur dans POST_DATA. Si l'on souhaite uploader un fichier php malveillant, il suffit de changer « application/octet-stream » en « image/jpg » il passera ainsi pour une image. Pour terminer le pirate n'a plus qu'à exécuter la page qu'il vient d'envoyer.

La seconde méthode s'appelle la double extension. En effet, on peut imaginer que pour se prémunir de la première méthode le programmeur a inclus un vérificateur d'extension. Une méthode pour contourner ce vérificateur consiste a créé une double extension par exemple *.php.gif. Il suffit d'ajouter un en-tête html et un *include*. Ainsi l'upload va fonctionner sans problème, vu qu'il s'agit d'un GIF. Après, il suffit de se rendre à son fichier et accéder aux données désirées.

### 2.5.10 Client qui nie avoir prolongé son abonnement au service

Il peut arriver qu'un client se retourne contre le propriétaire du site car son abonnement a été prolongé sans raison valable. On peut imaginer que cela soit le cas, mais cela peut également être une ruse dans le but d'obtenir un abonnement gratuit.

### 2.5.11 Des données disparaissent suite à une fausse manipulation du client

Prenons l'exemple d'un service web qui propose la gestion d'une équipe de sport. Au préalable l'utilisateur va devoir entrer toutes les données des joueurs. Si, par une fausse manipulation ou une erreur du client, les données venaient à disparaitre, cela pourrait entraîner du mécontentement.

### 2.5.12 Service inaccessible (client mécontent)

En cas d'attaques diverses sur la base de données ou sur les serveurs de l'hébergeur il est probable qu'un jour ou l'autre le site soit inaccessible. On s'attend donc très vite à une réaction négative des utilisateurs. En effet, si l'outil en ligne est devenu indispensable au client, il faut prévoir les foudres de celui-ci, sans compter qu'il pourrait exiger des dédommagements.

### 2.5.13 Accès physique aux serveurs

Un des points les plus importants dans la sécurité informatique et qui doit être mis en place dès le début est la sécurité dite physique. En effet, si des mots de passe ou des logiciels de cryptage existent, ils n'ont aucun intérêt si un individu peut accéder physiquement aux serveurs. Avec un accès physique, il est beaucoup plus facile de contourner la sécurité mise en place. Une personne avec de mauvaises intentions peut ainsi voler des données, les modifier ou alors tout simplement les effacer ce qui est dangereux pour l'intégrité, la confidentialité et la disponibilité du service web et de ses données.

Cette menace ne s'applique pas aux sites web qui hébergent leur site via des hébergeurs. En effet, ce sont les hébergeurs eux-mêmes qui garantissent la sécurité de leurs serveurs où sont stoquées les informations du client.

## 2.6 Mesure contre les menaces

### 2.6.1 Mesures

Dans cette partie les mesures contre les menaces définies précédemment sont définies.

#### *2.6.1.1 L'écoute des communications*

##### *2.6.1.1.1 IPSec*

Son utilisation la plus repondue est le « tunneling ». C'est une encapsulation qui permet de créer des réseaux VPN. On a ainsi, à travers un réseau non sécurisé ou public, une communication sécurisée

Voici le principe général de fonctionnement des tunnels crée par IPSec[5].

- Les données transitant sont chiffrées (confidentialité) et protégées (intégrité)
- Les 2 extrémités sont authentifiées
- Les adresses sources et destinations sont chiffrées, avec IPSec (IP dans IPSec)
- Ils peuvent présenter, suivant le protocole, des qualités anti-rejeux ou empêcher les attaques type man-in-the-middle.

5 SECURITEINFO.COM - IPSec : Internet Protocol Security (http://www.securiteinfo.com/cryptographie/IPSec.shtml) consulté le 12.05.2013

#### *2.6.1.2 La substitution de données*

### *2.6.1.2.1 Le chiffrement des données*

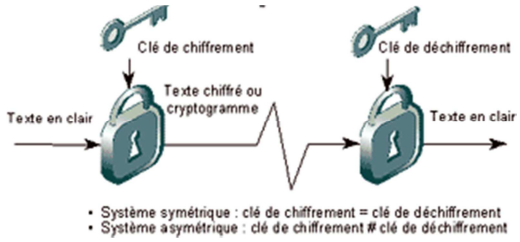


Figure 2

Comme on peut le voir dans la figure l'information est cryptée à son envoi et décryptée à la réception. Des règles mathématiques sont appliquées aux données en clair: une valeur d'entrée variable et secrète qui est combinée avec l'algorithme pour produire le message chiffré[6].

Il existe plusieurs types de chiffrement.

- Le chiffrement symétrique

  La même clé sert au chiffrement et au déchiffrement

- Le chiffrement asymétrique

  Une clé différente est utilisée pour le chiffrement et le déchiffrement

Dans tous les cas il est primordial que les clés restent stockées et qu'elles soient conservées comme des clés de serrure.

#### *2.6.1.3 Utilisation des bugs des applications*

### *2.6.1.3.1 Contrôler son code*

Dans le tableau des mesures on voit que celles qui doivent être appliquées sont de type palliatif et du domaine technique.

Ce genre de problème peut être dur à identifier pour le programmeur. En effet, les failles apparaissent peut-être que dans certains cas, qui n'ont pas été testé par le créateur du code. Il faut donc s'assurer que tous les tests de toutes les situations possibles sont réalisés.

[6]SECURITE-INFORMATIQUE.COM - le chiffrement des données – (http://www.securite-informatique.com/chiffrement.htm) consulté le 12.05.2013

#### 2.6.1.4 Déni de service et DDos

Il n'existe malheureusement pas de solution miracle pour ce type d'attaque. En effet, les requêtes malveillantes utilisent des ports "autorisés" ainsi que des paquets d'informations ressemblant de toute part à une demande d'un utilisateur honnête. Une des solutions connues est la méthode du flash-back[7] . La protection sera également différente si le contenu du site est stocké chez un hébergeur ou alors dans les locaux de l'entreprise. En effet, l'hébergeur est tenu de garantir le bon fonctionnement de ses serveurs.

##### 2.6.1.4.1 Flash-back

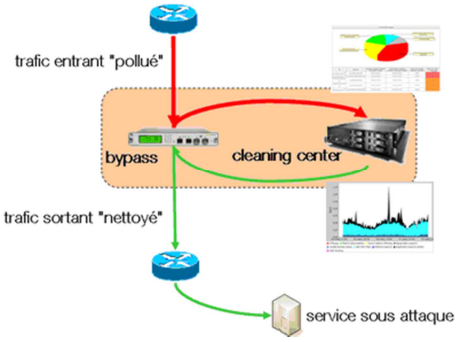


Figure 3

Cette méthode implémente des algorithmes de tri-sélectif du trafic. Le module flash-back est placé avant le poste de la « victime ». Le module fournit en sortie uniquement la partie purifiée.
Le module est doté d'une interface pour suivre la situation en temps réel et de paramétrer la protection en temps réel.

[7] SÉCURITE LE BLOG - lutte contre les attaques en DDoS : retour d'expérience (partie 1) (http://blogs.orange-business.com/securite/2009/02/lutte-contre-les-attaques-en-ddos-retour-dexperience-partie-1.html) consulté le 13.05.2013

#### *2.6.1.5 Attaques sur la base de données*

### *2.6.1.5.1 Utilisation de mysql_real_escape_string()*

La fonction « mysql_real_escape_string() » toute simple permet d'ajouter le caractère « \ » a différents caractères que voici [8]:

NULL, \x00, \n, \r, \, ', " et \x1a

Avec ce système on évite donc l'attaque comme présentée dans la description. Il suffit d'appliquer cette fonction à la variable avant de l'envoyer à la requête. Par exemple : `$nom = mysql_real_escape_string($_GET['nom']);`
Ainsi il est impossible de de modifier la requête car si la personne ajoute un " à la variable celui-ci sera précédé d'un « \ ». La faille est donc maîtrisée.

#### *2.6.1.6 Dévoiler des informations à un concurrent*

Etant donné que cette menace relève de l'erreur humaine, il n'y a pas de méthode miracle pour éviter tout problème.

### *2.6.1.6.1 Former le personnel*

Un des points les plus important pour éviter ce risque est de former le personnel à la sensibilité des informations qu'ils manipulent. Et surtout à respecter le secret professionnel lors de nouveaux modules en développement.

### *2.6.1.6.2 Validation des mails*

On pourrait imaginer pour les e-mails qui contiennent des pièces jointes, un système de validation. Le système de messagerie détecte les mails contenant un attachement et demande à l'utilisateur de confirmer les destinataires.

### *2.6.1.6.3 Protéger les documents*

Au même titre que le cryptage des données, une solution serait de protéger par mot de passe et de crypter les documents sensibles. Ainsi s'il y a une quelconque fuite, les données ne sont pas forcément exploitables

---

[8] http://www.siteduzero.com - Éviter les injections SQL - (http://www.siteduzero.com/informatique/tutoriels/eviter-les-injections-sql/securisation-1) - Consulté le 13.05.2013

#### *2.6.1.7 Copier-Coller malheureux*

### *2.6.1.7.1 Contrôler son code*

Une des solutions les plus logique est de contrôler son code. Il faut également être sûr de la source (forum privé d'entraide entre programmeurs par exemple). Et pour finir tester sous tous les angles le code issu du copier-coller.

### *2.6.1.7.2 Adapter le code*

Parfois, il est plus judicieux d'adapter le code au logiciel plutôt que de le prendre « tel-quel» et d'implanter des fonctionnalités inutilisées ou ne servant à rien.

#### *2.6.1.8 L'ingénierie sociale*

### *2.6.1.8.1 Prévention auprès des clients*

Le meilleur moyen de se prévenir contre cette menace est l'information aux clients. En effet, il est important de rappeler lors de l'inscription ou par mail que l'entreprise ne demandera jamais d'informations privées par mail. Ainsi les abonnés pourront directement détecter cette tentative de fraude s'ils reçoivent des mails demandant des informations bancaires, mot de passe ou toute autre information privée.

### *2.6.1.8.2 Site sécurisé*

Il est également important d'avoir un site web en https en tout cas lors des phases de paiement même s'il est conseillé que le site complet soit en https.
Il est également de votre devoir de rappeler les règles de base au niveau sécurité des sites web. Il faut rappeler au client de contrôler qu'il ne navigue pas sur un site http et non https.

#### *2.6.1.9 Input des clients risqués (image, fichier pdf)*

### *2.6.1.9.1 Liste de recommandation*

Voici une liste des principales actions pour se prémunir contre cette menace :

- ➔ Ne jamais se fier à ce que peut envoyer le client.
- ➔ Vérifier la configuration d'Apache afin d'agir en conséquence.
- ➔ Ne pas placer le .htaccess dans le répertoire d'upload
- ➔ Ne pas permettre l'écrasement de fichier
- ➔ Générer un nom aléatoire pour le fichier uploadé et enregistrer le nom dans une base de données.
- ➔ Ne pas permettre de voir l'index of du répertoire d'upload.
- ➔ Assigner les bonnes permissions au répertoire.
- ➔ Vérifier le mime-type avec getimagesize() et l'extension du fichier.[9]

#### *2.6.1.10 Client qui nie avoir prolongé son abonnement au service*

### *2.6.1.10.1 Contrat à l'inscription*

Il est primordial de faire accepter un contrat au client au moment de son inscription. Ainsi les différents points concernant les abonnements, leurs prolongations et la procédure pour se désabonner sont écrits noir sur blanc.

### *2.6.1.10.2 Log*

Pour pouvoir prouver sa bonne foi en cas de litige concernant les abonnements et leurs prolongations, il est important de conserver tous les détails des transactions dans un LOG. Ainsi le site ce couvre en cas de plainte d'un des clients.

[9] FUNINFORMATIQUE.COM - http://www.funinformatique.com/faille-upload-comment-lexploiter-et-sen-proteger-partie-1/ - PAGE 8 - Consulté le 20.02.2012

#### *2.6.1.11 Des données disparaissent suite à une fausse manipulation du client*

### *2.6.1.11.1 Backup*

Une des solutions consiste à sauvegarder les données de clients même après un effacement définitif de leurs parts. Ainsi, il est possible de restaurer et de rattraper la fausse manipulation

### *2.6.1.11.2 Interface utilisateur réactive*

Dans le cas où un utilisateur supprime un élément, il faut penser à demander confirmation à l'utilisateur pour la suppression et informer de manière claire l'action qui va suivre.
Exemple de Microsoft Online Services

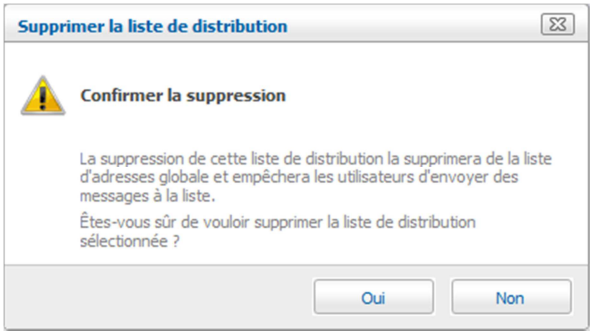


Figure 4

Ici on peut voir de manière claire ce que va entraîner la suppression d'un élément. L'utilisateur ne peut ainsi pas nier son action en cas de suppression.

#### *2.6.1.12 Service inaccessible (client mécontent)*

### *2.6.1.12.1 Plusieurs hébergeurs*

La solution la plus efficace pour se protéger contre cette menace est d'héberger le site en question et sa base de données chez plusieurs hébergeurs et dès l'ouverture du site celui-ci redirigera vers un des serveurs en état de marche.

#### *2.6.1.13 Accès physique aux serveurs*

Plusieurs types de mesures existent, j'ai sélectionné celles qui s'appliquent au cas d'un service web à partir d'une liste disponible sur le site « CASES – La sécurité de l'information pour tous ».[10]

### *2.6.1.13.1 Liste des mesures pour le cas d'un accès physique.*

- les identités des personnes puissent être surveillées dans les sas d'entrées et de sorties du bâtiment.
- les visiteurs et fournisseurs soient toujours accompagnés.
- les salles réservées aux serveurs soient verrouillées, et équipées de systèmes d'alarme, si besoin de caméras.

[10] CASES- LU https://www.cases.lu/mesures-de-securite-pour-pme-l-infrastructure-face-aux-menaces.html?&WCE_section_172_1=9&WCE_section_172_1=9&WCE_section_172_1=9#533 (Visité le 11.05.2013)

## *2.7 Tableau récapitulatif des mesures*

Pour commencer à établir les solutions pour palier à ces différentes menaces j'ai réalisé un tableau de classification des mesures. Pour réaliser ce tableau j'ai couplé les domaines et les types.

**Les domaines :**

- Techniques (Probabilité)
- Organisationnelles
- Humaines

**Les types :**

- Dissuasion
- Protection (Impact)
- Transfert (Impact)
- Palliatif (Impact)
- Prévention

| Mesures | Technique | Organisationnelle | Humaines |
|---|---|---|---|
| **Prévention** | TecPré | **OrgPré** | **HumPré** |
| **Dissuasion** | TecDis | OrgDis | HumDis |
| **Protection** | **TecPro** | OrgPro | **HumPro** |
| **Transfert** | TecTra | OrgTra | HumTra |
| **Palliative** | **TecPal** | OrgPal | HumPall |

Les mesures du tableau ci-dessus permettent de définir quelle mesure correspond à quelle menace. En gras les mesures identifiées dans mon tableau ci-dessous.

| N° | Menace | Mesure(s) |
|---|---|---|
| **1** | L'écoute des communications | TecPro |
| **2** | La substitution de données | TecPro |
| **3** | Utilisation des bugs des applications | TecPal – HumPré |
| **4** | Déni de service et DDoS | TecPro – OrgPré |
| **5** | Attaques sur la base de données | TecPro |
| **6** | Dévoiler des informations à un concurrent | HumPré |
| **7** | Copier-coller malheureux | HumPré - HumPal |
| **8** | l'ingénierie sociale | HumPré - TecPré |
| **9** | Input des clients risqués (image, fichier pdf) | TecPro |
| **10** | Client qui nie avoir prolongé son abonnement au service | OrgPré |
| **11** | Des données disparaissent suite à une fausse manipulation du client | HumPré |
| **12** | Service inaccessible (client mécontent) | TecPal |
| **13** | Accès physique aux serveurs | HumPro |

On peut constater que le domaine organisationnel n'apparait que très peu dans les mesures. Le principal domaine touché est le domaine technique. De plus les mesures sont pour la plupart liées à la protection ou à la prévention.

# 3. Evaluation des mesures

Maintenant que les menaces sont identifiées et leurs protections définies il faut passer au système de notation et d'évaluation. Le but de l'opération est de savoir si les mesures ont été mises en place.

Les critères qui ont été définis pour situer la sécurité du site en fonction des mesures sont les suivants : Oui, Non ou en partie

J'ai défini ces critères qui permettent d'évaluer assez facilement l'état de la sécurité de l'entreprise. J'ai préféré cette notation à la notation 1 sur 10 qui donne souvent des résultats arbitraires aux vues des choix de notes approximatifs.

Si l'entreprise possède déjà la protection décrite elle pourra cocher « Oui », si elle les a partiellement elle cochera « En partie » et finalement « Non » si celle-ci ne possède aucune protection contre la menace.

Dans la liste des 13 menaces ci-dessus il y'a 19 mesures établies en fonction de celle-ci.

Il est également demandé quels sont les objectifs au niveau sécurité pour l'entreprise. Ceci permet de mettre en avant les mesures les plus urgentes à prendre.

# 4. Livre blanc

Cette partie est un livre qui contient des recommandations et bonnes pratiques pour chaque mesure définie dans la partie précédente.

Dans cette partie je vais également établir une liste de questions pour permettre de jauger son business basé sur le web. Les 3 réponses possibles sont celles établies dans la précédente partie c'est-à-dire oui, non ou en partie. Ces questions sont l'outil d'évaluation pour les menaces décrites.

## *4.1 Recommandations*

### 4.1.1 L'Écoute des communications

Mesure définie : IPSEC identifiée comme une mesure de protection-technique

Cette mesure concerne la protection des communications entre un fournisseur et le client. Pour pouvoir garantir une sécurité maximale pour l'échange d'informations, il est judicieux de se protéger avec l'IPSEC. L'IPSEC est principalement utilisé avec le système de tunneling en créant des réseaux VPN. Le but de mon travail n'étant pas de définir l'IPSEC voilà les recommandations qui s'appliquent pour le cas d'un service web.

Il faut une protection de l'hôte à réseau. Il faut donc que les données et les adresses soient chiffrées à la source et la destination. Chaque partie prenant part à la communication doit également être authentifiée.

### 4.1.2 La substitution ou manipulation de données

Mesure définie : Chiffrer les données, c'est une mesure de protection-technique

Pour contrer à cette menace et appliquer la mesure il faut choisir le type de chiffrement.

Le chiffrement asymétrique est le plus sûr. En effet, une clé différente est utilisée pour chiffrer et déchiffrer.

### 4.1.3 Utilisation des bugs des applications

Mesure définie : Contrôler son code c'est une mesure technique palliative et également humaine de prévention.

Lors de l'utilisation de code clé en main il faut être sûr de ne garder que les parties utiles et ne pas laisser trainer des bouts de code qui ne sont pas utilisés. Il faut également s'assurer que le code ne contient pas de faille et qu'on a bien à disposition la dernière version. Un programmeur qui utilise un code clé en main a donc la responsabilité de s'assurer de la sécurité du code qu'il emprunte.

### 4.1.4 Déni de service et DDos

Mesure définie : Flas-Back de type technique de protection et organisationnel de prévention

Le meilleur moyen pour pouvoir profiter cette mesure est d'héberger sont site via un hébergeur qui propose cette protection.

### 4.1.5 Attaques sur la base de données

Mesure définie : Utiliser mysql_real_escape_string une mesure de type technique de protection.

Pour éviter des attaques sur la base de données il est important que les diverses requêtes sql soient sans faille.

Le risque ce manifeste lorsque l'on demande un input à l'utilisateur. Il est important d'appliquer une fonction de « nettoyage » ou de contrôle sur la valeur entrée par l'utilisateur avant d'y intégrer dans une requête. Ainsi on évite une attaque comme présentée dans la description de la menace.

### 4.1.6 Dévoiler des informations à un concurrent

Mesures définies : Prévention humaine via une formation du personnel, validation des mails et protection des documents.

Pour se protéger contre le risque de dévoiler des informations à un concurrent il faut que le personnel soit rigoureux et qu'il ne dévoile aucunes informations. Cette mesure étant purement humaine il est important d'avoir des employés de confiance.

Les documents et informations sensibles doivent être protégés, par exemple par un mot de passe. En effet, en cas de perte ou de vol de données il sera plus difficile d'obtenir les informations.

Les informations peuvent également être transmises par inadvertances via un courriel. La solution est un simple menu de validation de destinataire sur outlook ou autre système de messagerie permettant de valider les destinataires après avoir demandé l'envoi du mail.

### 4.1.7 Copier-coller malheureux

Mesure définie : prévention humaine et humaine palliative en contrôlant et adaptant le code.

Cette mesure concerne principalement les programmeurs. Il est important qu'ils soient sensibilisé au fait d'utiliser des code « tout fait ». En effet, en cas de réutilisation d'un code glané sur le web il faut être sûr de la provenance de celui –ci pour éviter toute mauvaise surprise. Il existe pour ceci des forums de professionnels qui s'échangent du code et pour lesquels l'inscription est payante. Avec ce système le contenu est validé et on a du code propre sans danger.

Il faut également que le code copié soit complètement utilisé. En effet, il faut l'adapter au logiciel et supprimer les parties inutiles pour éviter d'avoir des tests inutiles qui ralentissent l'exécution.

### 4.1.8 L'ingénierie sociale

Mesure définie : prévention humaine et prévention technique

Pour protéger le service web il faut que celui-ci soit en https. Ainsi si une copie du site est réalisée celle-ci n'aura pas le certificat de sécurité et permet donc de rendre attentif l'utilisateur et ainsi éviter de tomber dans le piège.

Il faut également faire de la prévention auprès des utilisateurs et les informer clairement que votre site ne demandera jamais d'informations privées.

### 4.1.9 Input des clients risqués (image, fichier pdf)

Mesure définie : protection technique

Pour cette mesure il existe une série de recommandations que j'ai établies dans la description de la menace.

Pour tout upload il est important que les dossiers d'upload soient sécurisés et qu'il soit uniquement possible de mettre des fichiers du type demandé. Une fonction/procédure de vérification est nécessaire.

En procédant de cette manière seuls les fichiers validés sont enregistrés sur le serveur.

### 4.1.10 Client qui nie avoir prolongé son abonnement au service

Mesure définie : Organisation et technique de prévention

Le client doit accepter un contrat pour pouvoir s'inscrire et utiliser le site. Il faut que ce contrat soit clair et précis et qu'il couvre toutes les possibilités de recours. En effet, en cas de prolongation automatique d'abonnement il faut que ceci soit spécifié à l'inscription.

Dans une autre mesure si le client nie avoir prolongé l'abonnement, il est utile d'avoir un LOG qui retranscrit les actions du client et permet de prouver que la prolongation vient de sa part.

### 4.1.11 Des données disparaissent suite à une fausse manipulation du client

Mesure définie : Prévention humaine via une interface utilisateur réactive et des backups.

Le service web doit posséder de solide backup pour pouvoir récupérer les données. Pour éviter une fausse manipulation au client, il faut un système de confirmation de suppression ainsi l'utilisateur accepte son action.

De plus, lors de la suppression effectuée par un utilisateur il faut désactiver les informations (pour que les données ne soient pas affichées) plutôt que de les retirer de la base.

### 4.1.12 Service inaccessible (client mécontent)

Mesure définie : Technique palliative en utilisant différents hébergeurs.

La mesure constitue à rediriger l'utilisateur dès l'ouverture du site ou d'une page vers un serveur fonctionnel. La gestion de la redirection n'est pas visible pour l'utilisateur. En procédant ainsi le service web redirige directement vers un serveur fonctionnel.

### 4.1.13 Accès physique aux serveurs

Mesure définie : Protection humaine avec diverses mesures

Cette mesure consiste à avoir une liste précise et limite des personnes ayant accès physiquement aux serveurs. Il faut également que la salle des serveurs soit sécurisée et surveillée.

Dans le cas où le service web est entièrement stocké chez un hébergeur, c'est l'hébergeur qui garantit la sécurité des données.

## *4.2 Questionnaire*

### 4.2.1 Partie « Objectif »

Dans cette partie le but est de définir les objectifs au niveau sécurité pour un service web.

La note de 1 indique que cela a une faible importance la note 5 indique une haute importance.

| N° | Question | Note (1-5) |
|---|---|---|
| 1 | Le service doit-il être constamment accessible ? | |
| 2 | Les données doivent-elle être exactes et protégées ? | |
| 3 | Les informations du site ne doivent pas être rendues disponibles ou divulguées à des personnes non autorisées ? | |
| 4 | Le fait de pouvoir prouver l'implication d'un client dans une action est important pour votre service ? | |

### 4.2.2 Partie « Evaluation »

| N° | Question | Oui | Non | En partie |
|---|---|---|---|---|
| 1 | Les communications sont-elles protégées à l'aide d'IPSEC ? | | | |
| 2 | L'échange de données se fait-il avec des chiffrements asymétriques ou symétriques ? | | | |
| 3 | Lors de l'utilisation d'application toute faite le code est-il systématiquement contrôlé ? | | | |
| 4 | L'hébergeur du site fournit-il une protection contre le déni de service et DDos ? | | | |
| 5 | La fonction mysql_real_escape_string() est utilisée dans le code ? | | | |
| 6.1 | Le personnel est-il au courant de la sensibilité des informations qu'il manipule ? | | | |
| 6.2 | Lors de l'envoie de mail un contrôle est-il effectué sur les pièces jointes ? | | | |
| 6.3 | Les documents comprenant des informations sensibles sont-ils protégés par un mot de passe ? | | | |
| 7.1 | Le code est-il testé systématiquement lors d'un copier-coller d'un code depuis une source externe ? | | | |
| 7.2 | Lors de l'utilisation d'un code externe celui-ci est-il systématiquement adapté ? | | | |
| 8.1 | Lors de l'inscription il y'a-t-il une information transmise aux clients contre le risque de l'ingénierie sociale ? | | | |
| 8.2 | L'accès au site ce fait via https ? | | | |
| 9 | Un contrôle est-il fait lors de l'upload de fichier par le client sur le serveur ? | | | |
| 10.1 | Un contrat clair et précis est affiché lors de l'inscription et dois être accepté par l'utilisateur ? | | | |
| 10.2 | Un log de toutes les actions des utilisateurs est enregistré ? | | | |
| 11.1 | Le site dispose d'un système de backup ? | | | |
| 11.2 | Le site dispose d'une interface utilisateur réactive | | | |
| 12 | Le site est-il hébergé chez plusieurs fournisseurs ? | | | |
| 13 | Les locaux des serveurs sont-ils surveillés et leurs accès limités ? | | | |

# 5. Cas SoSport

La première partie du questionnaire concerne les objectifs visés par la PME. Le but étant de savoir quels sont les priorités de l'entreprise concernant les dimensions suivantes :

- Disponibilité
- Intégrité
- Confidentialité
- Non-répudiation

Voici les résultats obtenus pour le site SoSport :

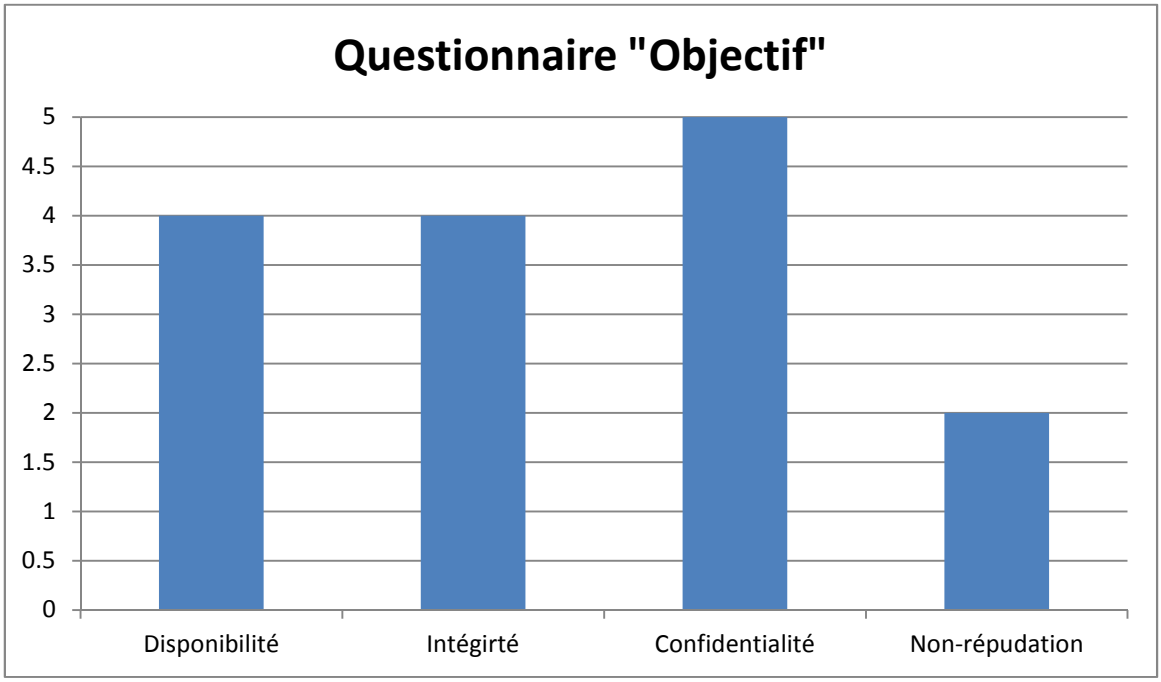


Figure 5

La seconde partie du questionnaire concerne l'état des mesures à prendre.
On cherche à savoir lesquelles sont mises en place ou en partie et les quelles sont encore inexistantes. En réalisant le questionnaire pour certaines questions, il peut arriver que la personne qui répond ne connaisse pas l'état concernant cette mesure c'est pourquoi la réponse « Ne sais pas » apparait dans le tableau.

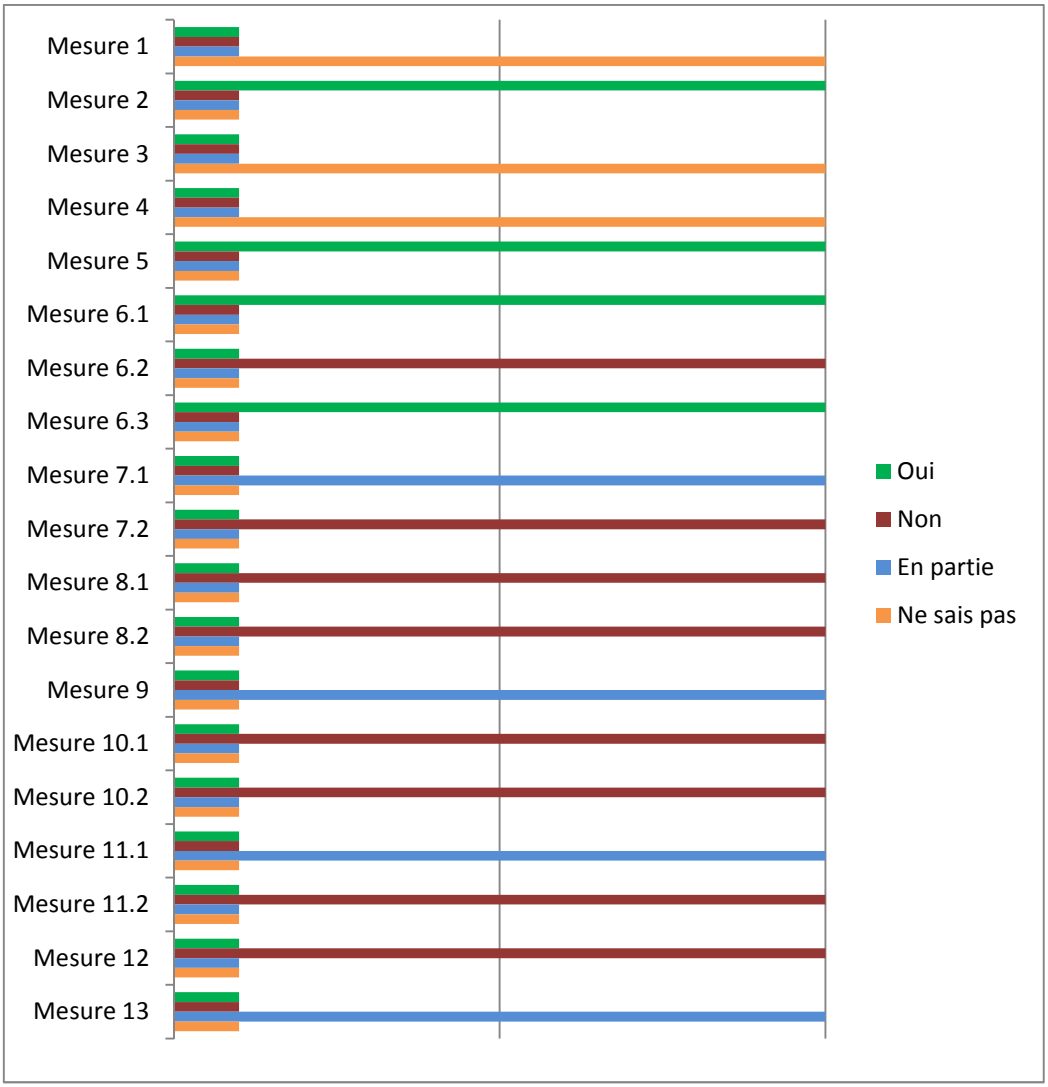


Figure 6

Pour analyser les réponses, j'ai séparé les mesures par dimension de la menace qu'elle concerne (identifiées chapitre 2.4).

**Intégrité et confidentialité :**

Mesure 1 :

Pour cette mesure aucune réponse n'a été fournie. Il faut donc partir sur le fait que cette mesure n'est pas en place et qu'il faut donc y remédier.

Mesure 2 :

L'échange des données se fait de façon asymétrique pour le cas SoSport. La mesure est donc en place.

**Disponibilité, intégrité et confidentialité :**

Mesure 3 :

Pour cette mesure pas de réponse fournie. En effet, il se peut que certaines PME n'utilisent pas d'application toute faite. Ce n'est donc pas une menace pour SoSport.

Mesure 4 :

Tout comme pour la mesure 1 pas de réponse fournie. Du fait que SoSport est stoqué sur un hébergeur externe c'est à celui-ci de mettre la mesure en place.

Mesure 5 :

La mesure est en place.

Mesure 7.1 :

Cette mesure est en partie mise en place. Cette menace étant du domaine « humain » il faut donc rappeler aux programmeurs les risques et effectuer des contrôles systématiquement pour être totalement à l'abri. Utiliser des forums de professionnels de l'informatique peut être une solution qui permet d'être plus « léger » sur les contrôlés.

Mesure 7.2 :

Tout comme pour la mesure précédente il faut dans la mesure du possible adapter le code à son environnement pour éviter des calculs trop longs et surtout inutiles.

Mesure 9 :

Une partie de cette mesure est en place grâce au framework qui effectue des contrôles sur les ficher uploader.

Mesure 13 :

Cette mesure ne concerne pas SoSport car le site n'est pas héberger dans leurs locaux.

**Confidentialité :**

Mesure 6.1 :

La mesure est en place.

Mesure 6.2 :

Cette mesure n'est pas mise en place. Cette mesure étant très radicale et ralentissant les échanges, ce qui explique que peu de PME l'utilise. Il est cependant important de vérifier à plusieurs reprises si l'on envoie uniquement les informations nécessaires.

Mesure 6.3 :

La mesure est en place.

Mesure 8.1 :

Pour le site SoSport il n'y a aucune mesure concernant l'ingénierie sociale.

Mesure 8.2 :

L'accès au site ce fait via http et non https. Il est préférable d'avoir un site en https pour de raisons évidentes de sécurité et également pour rassurer les utilisateurs surtout sur une plateforme web dont les accès sont régulés par un abonnement.

**Non-Répudiation :**

Mesure 10.1

En ce qui concerne cette mesure on peut voir qu'il n'y pas de contrat d'utilisation présenté à l'utilisateur lors de l'inscription.

Mesure 10.2

Les diverses actions des utilisateurs ne sont pas regroupées dans un log. Il est donc difficile de prouver ou nier une action d'un utilisateur

Mesure 11.1

Le back-up s'effectue en partie via le code.

Mesure 11.2

Lors de la suppression d'éléments il n'y pas de confirmation de l'utilisateur.

**Disponibilité :**

Mesure 12 :

L’hébergement ce fait chez un fournisseur. En cas de problème chez eux le site est donc inaccessible.

**Conclusion du cas concret :**

Pour le site SoSport qui a la totalité de son business en ligne il y a certaines mesures en place mais une bonne partie qui ne le sont pas.

Pour certaines menaces, il n’y pas d’urgence immédiate et des mesures peuvent être prises dans le futur. Pour certaines, il s’agit de l’hébergeur qui les gèrent directement.

Suite au premier questionnaire, on voit que c’est la confidentialité qui est le plus importante pour SoSport car la note d’importance 5 a été indiquée.

Les mesures à prendre le plus rapidement possible sont la 8.1 et 8.2 c’est à dire que le site soit en https et que les clients soient prévenus des risques et de les briffer sur le fait d’envoyer des informations personnelles n’est jamais demandé par SoSport.

Un notre point à relever est qu’au niveau de la non-répudiation, qu’il existe le plus de faille et l’on peut constater que SoSport ne se protège pas assez contre les utilisateurs. En effet, il n’y a pas de contrat à l’inscription entre les utilisateurs, il n’y pas de log et également pas de confirmation de suppression. En cas de plainte d’un utilisateur, il sera difficile de prouver qui a raison. Etant donné la note de 2 choisie par SoSport pour la non-répudiation on comprend pourquoi beaucoup de mesures dans ce domaine ne sont pas encore prisent.

Pour finir on peut voir aux vues des réponses obtenues que les menaces techniques sont pour la plupart couvertes soit par SoSport soit par son hébergeur.

# 6. Conclusion

A la fin de ce travail, mes recherches me permettent de dire qu'il existe en grand nombre de menaces pour les PME qui ont leur business basé en ligne.

Souvent dans ce type de business les sites sont créés soit par entrepreneurs qui ne connaissent pas grand-chose à l'informatique, soit par des informaticiens qui ne connaissent pas grand-chose à la gestion des risques humains. C'est pourquoi il est important d'avoir des personnes compétentes dans tous les domaines pour garantir une sécurité maximale au business.

De nombreuses menaces existent et ce travail reprend une grande partie de celles-ci. Il est clair et non évitable que de nouvelles menaces fleurissent jour après jour. Ceci, grâce à l'imagination et l'appât du gain des hackers. C'est pourquoi il est important d'être réactif.

Ce travail m'a permis de voir un grande partie des menaces pour une entreprise qui à son business en ligne et également de chercher ou créer des mesures pour palier à ces diverses menaces.

En ayant pu réaliser un questionnaire qui a été rempli par une entreprise qui était dans la situation précise de mon travail, m'a permis de me rendre compte que certaines mesures qui me paraissaient évidentes n'ont pas été mises en place.

Cela montre donc que ce carnet blanc réalisé est utile, et que ce travail peut servir de base pour une version plus complète, qui s'adapte au fur et à mesure de l'avancée de la technologie et des méthodes des pirates.

# 7. Bibliographie

ORGANISATION INTERNATIONALE DE NORMALISATION. Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire. Genève : ISO, 2009. 57 p. Norme internationale ISO/CEI 27000 : 2009

WIKIPEDIA - Attaque par déni de service (http://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service) consulté le 12.05.2013

CERTA - Le déni de service distribué (http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001) consulté le 13.05.2013

LAMELEE.COM - http://www.lamelee.com/les-ressources/securite-de-linformation/securite-des-systemes-dinformation/view.html - PAGE 8 - Consulté le 11.05.2012

WIKIPEDIA - Attaque par déni de service (http://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service) consulté le 12.05.2013

[1]SECURITE-INFORMATIQUE.COM - le chiffrement des données – (http://www.securite-informatique.com/chiffrement.htm) consulté le 12.05.2013

CERTA - Le déni de service distribué (http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001) consulté le 13.05.2013

SÉCURITE LE BLOG - lutte contre les attaques en DDoS : retour d'expérience (partie 1) (http://blogs.orange-business.com/securite/2009/02/lutte-contre-les-attaques-en-ddos-retour-dexperience-partie-1.html) consulté le 13.05.2013

SITEDUZERO.COM - Éviter les injections SQL - (http://www.siteduzero.com/informatique/tutoriels/eviter-les-injections-sql/securisation-1) - Consulté le 13.05.2013

FUNINFORMATIQUE.COM - http://www.funinformatique.com/faille-upload-comment-lexploiter-et-sen-proteger-partie-1/ - PAGE 8 - Consulté le 20.05.2013

CASES- LU https://www.cases.lu/mesures-de-securite-pour-pme-l-infrastructure-face-auxmenaces.html?&WCE_section_172_1=9&WCE_section_172_1=9&WCE_section_172_1=9#533 (Visité le 11.05.2013)

SECURITEINFO.COM - IPSec : Internet Protocol Security (http://www.securiteinfo.com/cryptographie/IPSec.shtml) consulté le 12.05.2013