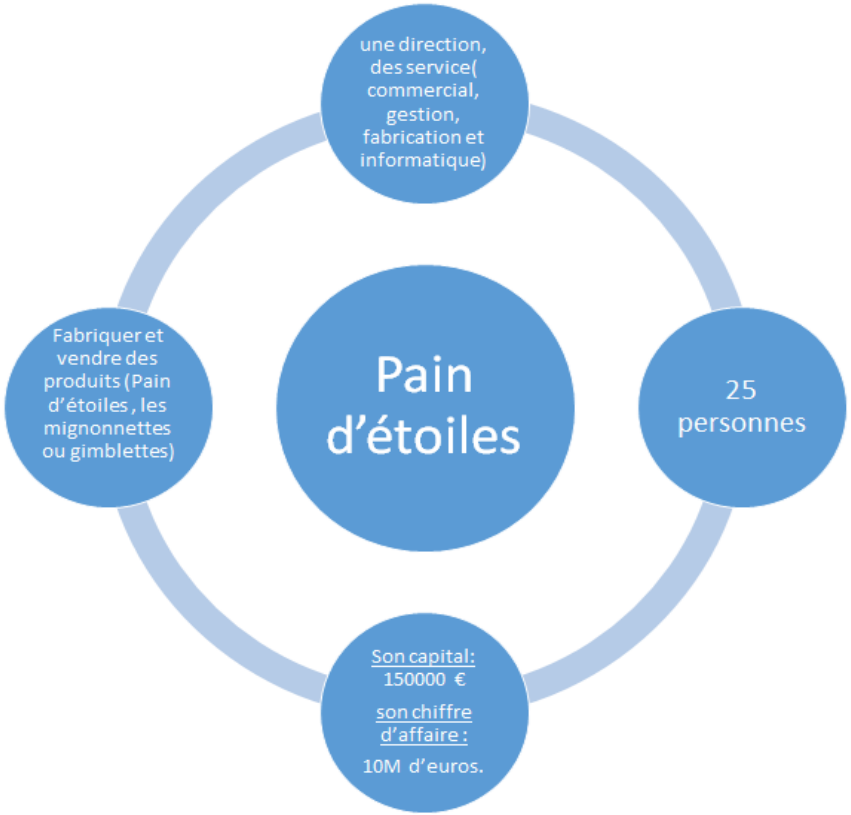
“Sécurité des systèmes d’information”

Équipe 2

POLYTECH MARSEILLE
Aix+Marseille Université

Sommaire

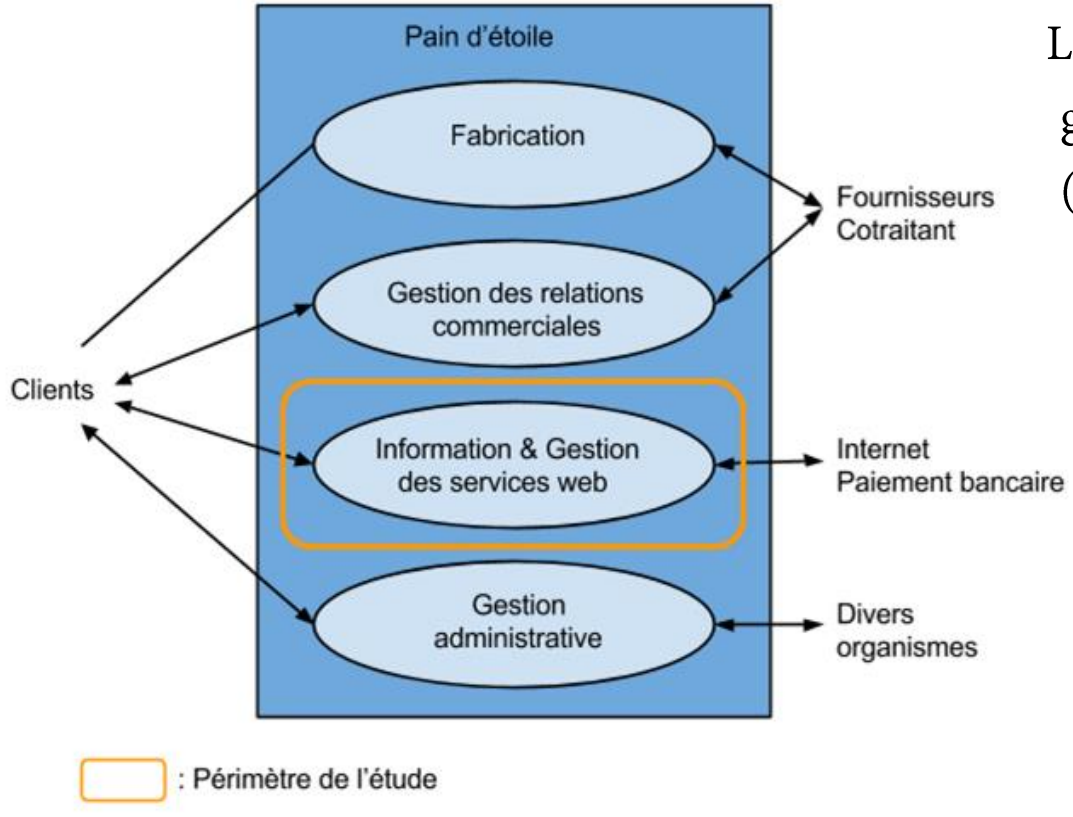
Le cadre d'études des risques



Objectif

Cartographie des risques avec l'établissement de mesures de sécurité afin de vérifier qu'elle n'est pas soumise à des risques non maîtrisés.

Périmètre d'étude



Le périmètre de l'étude se porte sur la gestion des commandes faites par internet (depuis 2 ans).

Nous avons les processus :

-Gestion des services Web

-Mise à jour du site Web

Les menaces retenues

les menaces sont souvent liées à

- des erreurs humaines
- des erreurs d'implémentation des systèmes
- La négligence du personnel
- l'introduction d'un virus.

Types de sources de menaces	Exemples
Source humaine externe, malveillante, avec de faibles capacités	Personnel de nettoyage (soudoyé)
Source humaine externe, malveillante, avec des capacités importantes	Concurrent
Source humaine externe, malveillante, avec des capacités illimitées	Pirate informatique
Source humaine interne, sans intention de nuire, avec de faibles capacités	Employé peu sérieux
Source humaine interne, sans intention de nuire, avec des capacités importantes	Informaticien
Source humaine interne, sans intention de nuire, avec des capacités illimitées	DSI
Virus non ciblé	Virus non ciblé
Catastrophe naturelle ou sanitaire	Maladie, Inondation

Les événement redoutes

Niveau de gravité

- ❑ Limitée
- ❑ Importante
- ❑ critique

Evénement redouté
Indisponibilité su site web pendant plus d'une heure entrainant une perte financière
Indisponibilité des coordonnées des clients empêchant l'envois de la commande
Indisponibilité de la base de données plus d'une heure
Divulgation des coordonnées des clients entrainant une perte de confiance
Atteinte a la confidentialité de la base de données entrainant la perte d'image de marque
Altération du site empêchant la bonne prise de commande
Altération des coordonnées clients entrainant des erreurs de livraison
Altération de la base de données empêchant la gestion de commande
Accès au site web public

Risques analysés

8 risques :

- Gravité et vraisemblance variable selon le risque.
- Sans mesure/Avec mesures/Avec mesures complémentaires .
- Exemple montrant un résultat.

Évaluer les risques

1. Estimation sans mesure

Gravité : **Critique**

Vraisemblance : **Forte**

2. Estimation avec mesures existantes

Gravité : **Critique**

Vraisemblance : **Significative**

3. Estimation avec mesures complémentaires

Gravité : Critique

Vraisemblance : Minime

Evènement redouté

Bien essentiel	Critère	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Base de données	Disponibilité	Moins de 1h	Pirate Employé peu sérieux Panne Informaticien Phénomène naturel Concurrent Virus non ciblé Innondation	Perte de crédibilité Perte de notoriété Impossibilité d'assurer ou Perte de données Perte de marchés	Critique

Scénarios de menace | **Mesure(s) de sécurité**

+ **Ajouter une mesure de sécurité**

Etat (E/C)	Libellé	Type de mesure	BS associé
C	Ajout d'anti-virus	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Salle INFO. Serveur Apache
C	Doubler les équipements	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Switch

Évaluer les risques

Gravité / Vraisemblance	1.Minime	2.Significative	3.Forte	4.Maximale
4.Critique		R 2	R 5	
3.Importante		R 1	R 6	
2.Limitée		R 0 R 1 R 2	R 4 R 7	
1.Négligeable		R 0 R 3 R 4		

Les mesures déjà mises en place

3 types de mesure :

- Prévention
- Protection
- Récupération

Libellé	Type de mesure	BS associé	P	Prc	Réc
Dispositifs de protection par badge	Mesures issues d'un référentiel	Badge Badgeuse	X	X	
Sauvgarde de données sur un disque externes	Mesures issues d'un référentiel	Disques externes			X
Alimentation de secours	Mesures issues d'un référentiel	Alimentation de secours		X	
Dispositif de lutte contre l'incendie	Mesures issues d'un référentiel	Dispositif de détection/extinctior		X	
Refroidir le matériel	Mesures issues d'un référentiel	Climatisation		X	
Remplacement de l'ingénieur du réseau	Mesures issues d'un référentiel	(DSI)	X		
Protection des postes de travail dans les ateliers	Mesures issues d'un référentiel	Pare-feux		X	
Afficher les consignes de protection	Mesures issues d'un référentiel	(DSI) (COM)-Kiroule Pierre (INF) INgénieur Réseau (INF) (COM)	X		
Contrat d'assurance	Mesures issues d'un référentiel	Serveur de base de données My Serveur d'applications Ordinateurs pour les ateliers Serveur DNS Serveur de messagerie Serveur Apache			
Antivirus	Mesures issues d'un référentiel	Ordinateurs pour les ateliers		X	
Répartir les charges	Mesures issues d'un référentiel	Répartiteur Foundry	X		

Les objectifs de sécurité :

1. choix des options de traitement :

Risques	Objectifs de sécurité	Commentaires
Indisponibilité de la base de données plus d'une heure	Réduire	effectuer des sauvegardes régulières permettant sa récupération dans des brefs délais
Indisponibilité du site web plus qu'une heur	Réduire	Former les responsable du site a fin qu'il interviennent plus rapidement.
Divulgation des coordonnes des clients entraînant une perte de confiance	Réduire	Crypté les informations relatif au client

Les objectifs de sécurité

2. Analyse des risques résiduels:

Les métriques retrouvé pendant l'analyse de risque :

- Niveaux de gravité :

Négligeable	La société surmontera les impacts sans difficulté
Limitée	La société surmontera les impacts malgré quelques difficultés
Importante	La société surmontera les impacts avec de sérieuses difficultés

- Niveaux de vraisemblance :

Significative	Cela pourrait se (re)produire.
Forte	Cela devrait se (re)produire un jour ou l'autre.

Les objectifs de sécurité

2. Analyse des risques résiduels:

Risques	Gravité	Vraisemblance
Indisponibilité de la base de donné plus d'une heure	Limité	Significative
Indisponibilité du site Web plus qu'une heur	Limité	Forte
Divulgation des coordonnes des clients entraînant une perte de confiance	Importante	Significative
Altération des coordonnées clients entraînant des erreurs de livraison	Négligeable	Forte

Les mesures à mettre en place

Types de mesures:

- 1ère => Prévention
- 2ème => Protection
- 2ème & 4ème => Récupération

Liste des mesures de sécurité - 15 élément(s)

Etat (E/C) 1 ▲	Libellé	Type de mesure	BS associé
C	Doubler les équipements	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Switch Onduleur Serveur Apache
C	Ajout d'anti-virus	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Salle INFO. Serveur Apache
C	Système de correction des erreurs	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Serveur Apache
C	Mise en place d'un système de sauvegarde RAID 1	Mesures de l'étude	Serveur de base de données MySql Serveur d'applications Serveur DNS Serveur de messagerie Serveur Apache Serveur Apache

MERCI POUR VOTRE **ATTENTION**

AVEZ - VOUS DES QUESTIONS ?