ÉTUDE EBIOS

CloseNell

Gael Huot - Thibaud Jeannin - Nathan Piranda

Module 1 : Étude du contexte

Rappel des notions importantes définies en TD

1.1 Cadre de l'étude des risques

1.1.5 Identification des sources de menaces

	Malveillant	Non-malveillant
Humain - Interne	Conflits internes	Employé maladroit
Humain - Externe	Employé d'un prestataire Entreprises concurrentes Clients conflictuels Pirates	Employé d'un prestataire Client peu familiarisé avec la sécurité
Non-humain	Catastrophes naturelles Maladies/épidémies Accidents Liés au bâtiments	

1.2 Mise en place des métriques

1.2.1 Critères de sécurité et échelles de besoins

Disponibilité	Description (durée)
Intolérable	> 48h
Tolérable	6 - 48h
Contractuelle	4 - 6h
Objectif interne	3 - 4h
Immédiat	< 3h

Intégrité	Description
Indétectable	Pas intègre, sans possibilité de vérifications
Détectable	Pas intègre, mais la corruption est détectable
Maîtrisé	Pas intègre, mais peut être corrigé

Intègre	Intègre
Confidentialité	Description
Privé	Disponible qu'à une partie du personnel et/ou des partenaires identifiés
Réservé	Accessible qu'au personnel
Limité	Disponible qu'au personnel et aux partenaires identifiés
Public	Accessible à tout le monde

1.2.2 Echelle de niveaux de gravité

Description	
Critique	Conduira à la fermeture de la société
Important	Fermeture de la branche de la vente aux particuliers avant deux ans Avenir incertain de la société
Limité	La vente aux particuliers est juste rentable Avenir incertain de la vente aux particuliers
Négligeable	Ne mettra pas en cause la stabilité financière de la société

1.2.3 Echelle de vraisemblance

Description	
Minime	Cela ne devrait pas se (re)produire
Significative	Cela pourrait se (re)produire
Forte	Cela devrait se (re)produire un jour
Maximal	Cela va certainement se (re)produire prochainement

Module 2 : Étude des événements redoutés

2.1 - Analyser les événements redoutés

Evénements redoutés	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Etablir des factures				
Indisponibilité de factures	Disponibilité : Intolérable	- Problème technique - Pirate - Employé maladroit	- Retard de traitement des commandes - Perte de crédibilité	Négligeable
Altération de factures	Intégrité : Détectable	- Problème technique - Employé maladroit - Pirates	- Perte de crédibilité - Retard de traitement des commandes - Perte de chiffre d'affaire - Pénalités	Limité
Site internet				
Indisponibilité du site internet	Disponibilité: Contractuelle	- Problème technique - Pirates - Employé maladroit	- Perte de crédibilité - Perte de clients	Limité
Compromission du contenu du site internet.	Intégrité : Détectable	- Employé maladroit - Employé malveillant - Pirates	- Perte de crédibilité - Perte de clients - Dépenses imprévues	Important
Visualisations				
Compromission de visualisations	Intégrité : Détectable	- Pirates - Employé malveillant	- Perte de crédibilité	Important
Altération de visualisations	Intégrité : Maîtrisé	- Pirates	- Perte de crédibilité - Perte de clients	Limité
Données anonymisées				
Divulgation des données anonymisées	Confidentialité : limité	- Pirates - Employé malveillant - Employé du prestataire malveillant	- Perte de crédibilité - Perte de clients - Pénalités	Limité
Données désanonymisées				
Divulgation des données désanonymisées	Confidentialité : privé	- Pirates - Employé malveillant - Employé du prestataire malveillant	- Perte de crédibilité - Pénalités	Critique
Catalogue				
Indisponibilité du catalogue	Disponibilité : Contractuelle	- Pirate - Employé peu sérieux	- Perte de crédibilité - Perte de clients	Limité
Altération du catalogue	Intégrité : Détectable	- Pirate - Employé peu sérieux - Employé malveillant	- Perte de crédibilité - Indisponibilité du catalogue	Important

2.2 - Évaluer chaque événements redoutés

Gravité	Evénements redoutés
4.Critique	- Divulgation des données désanonymisées
3.Importante	- Compromission du contenu du site internet. - Compromission de visualisations - Altération du catalogue
2.Limitée	- Divulgation des données anonymisées - Altération de factures - Indisponibilité du site internet - Altération de visualisations - Indisponibilité du catalogue
1.Négligeable	- Indisponibilité de factures

Module 3 : Étude des scénarios de menaces

3.1 - Analyser les scénarios de menaces

Scénarios de menaces	Sources de menaces	Vraisemblance
Organisation de l'entreprise		
Menaces sur l'entreprise CloseNell causant une indisponibilité	- Employé maladroit - Employé malveillant	Significative
Menaces sur l'entreprise CloseNell causant une altération	- Employé maladroit	Forte
Menaces sur l'entreprise CloseNell causant une compromission	- Conflits internes	Minime
Catalogue		
Altération du catalogue	- Pirate - Employé peu sérieux - Employé malveillant	Significative
Indisponibilité du catalogue	- Pirate - Employé peu sérieux	Forte
PC Portable marketing		
Accès non autorisé	- Employé malveillant - Employé peu sérieux - Conflits internes - Employé d'un prestataire	Forte
Panne / Casse	- Employé malveillant - Employé peu sérieux - Conflits internes - Employé d'un prestataire	Forte
Vol	- Conflits internes - Employé malveillant	Significative
Virus	- Pirate - Employé peu sérieux	Forte
Accès non autorisé à distance	- Pirate - Employé malveillant - Employé d'un prestataire	Significative
Serveurs réseaux OVH		
Panne	- Pirate - Employé d'un prestataire - Liés au bâtiment	Forte
Serveurs site Internet		
Attaque	- Pirate	Significative
Mauvaise configuration	- Employé d'un prestataire	Significative

3.2 - Évaluer chaque scénario de menaces

Vraisemblance	Scénarios de menaces
Maximale	
Forte	- Menaces sur l'entreprise causant une altération - Indisponibilité du catalogue - Accès non autorisé - Panne / Casse - Virus - Attaque
Significative	- Menaces sur l'entreprise causant une indisponibilité - Altération du catalogue - Vol - Accès non autorisé à distance - Panne - Mauvaise configuration
Minime	- Menaces sur l'entreprise causant une compromission

Module 4 : Étude des risques

4.1 - Apprécier les risques

- R1 : Risques liés à l'indisponibilité de factures au delà de 48h
- R2 : Risques liés à l'intégrité des factures pour lesquelles une corruption doit être détectable
- R3 : Risques liés à l'indisponibilité du site internet au delà de 6h
- R4 : Risques liés à l'intégrité des visualisation du site web pour lequel une corruption doit être détectable
- R5 : Risques liés à la confidentialité des données anonymisées qui doivent rester accessibles seulement au personnel et aux partenaires
- R6 : Risques liés à la confidentialité des données désanonymisées au delà d'une partie du personnel et des partenaires identifiés
- R7 : Risques liés à la disponibilité du catalogue qui doit rester disponible sous 6 heures
- R8 : Risques liés à l'intégrité du catalogue pour lequel une corruption doit être détectable

		Vraisemblance			
		Maximale	**Forte**	**Significative**	**Minime**
Gravité	**Critique**	R6			
	Important	R8		R4, R5	
	Limité	R2, R3, R7			
	Négligeable	R1			

Risques négligeables	**Risques significatifs**	**Risques intolérables**

4.2 - Identifier les objectifs de sécurité

4.2.1 - Choisir les options de traitement des risques

Pour chaque risque, il y a 4 traitements réalisables, nous pouvons :

- Éviter le risques, c'est-à-dire changer le contexte de telle sorte qu'on ne soit plus exposé au risque.
- Réduire le risques, c'est-à-dire prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance du risque.
- Prendre le risque, c'est-à-dire assumer les conséquences sans prendre de mesures de sécurité supplémentaires.
- Transférer le risque, c'est-à-dire partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un ou plusieurs tiers.

Risque	Evitement	Réduction	Prise	Transfert
R1 : Indisponibilité des factures			✓	
R2 : Intégrité des factures		✓		
R3 : Disponibilité du site internet		✓		
R4 : Intégrité du site internet		✓		
R5 : Confidentialité des données anonymisées	✓			
R6 : Confidentialité des données désanonymisées	✓			
R7 : Disponibilité du catalogue			✓	
R8 : Intégrité catalogue		✓		

4.2.2 - Analyser les risques résiduels

Risque résiduel	Gravité	Vraisemblance
R1 : Indisponibilité des factures	Négligeable	Forte
R2 : Intégrité des factures	Limité	Forte
R3 : Disponibilité du site internet	Limité	Forte
R4 : Intégrité du site internet	Important	Significative
R7 : Disponibilité du catalogue	Limité	Forte
R8 : Intégrité catalogue	Important	Forte

Module 5 : Études des mesures de sécurité

5.1 – Formaliser les mesures de sécurité à mettre en œuvre

5.1.1 - Déterminer les mesures de sécurité

Mesures de sécurité	R1	R2	R3	R4	R5	R6	R7	R8	Bien support	Préventio	Protection	Récupérat
Renforcer les contraintes sur le contrat du prestataire			✓		✓	✓			Prestataire bancaire	✓	✓	
Chiffrer les données sensibles						✓	✓					
Signer les données avec une clé privée					✓			✓	Serveur du site		✓	
Sécurisation des échanges entre serveur ERP et serveur site					✓	✓			Réseau OVH		✓	
Sauvegarde	✓	✓		✓				✓	Serveur			✓
Changer régulièrement les mots de passe.		✓		✓	✓	✓		✓	Tout	✓		
Organiser une conférence sur la sensibilisation à la sécurité en entreprise.	✓	✓		✓	✓	✓	✓	✓	Tout	✓		

5.1.2 - Analyser les risques résiduels

Risque 1 : Risques liés à l'indisponibilité de factures au delà de 48h				
Gravité	**Négligeable**	Limitée	Importante	Critique
Vraisemblance	Minime	Significative	**Forte**	Maximale

Risque 2 : Risques liés à l'intégrité des factures pour lesquelles une corruption doit être détectable				
Gravité	**Négligeable**	~~**Limitée**~~	Importante	Critique
Vraisemblance	Minime	**Significative**	~~**Forte**~~	Maximale

Risque 3 : Risques liés à l'indisponibilité du site internet au delà de 6h				
Gravité	Négligeable	**Limitée**	Importante	Critique
Vraisemblance	Minime	**Significative**	~~**Forte**~~	Maximale

Risque 4 : Risques liés à l'intégrité des visualisation du site web pour lequel une corruption doit être détectable				
Gravité	Négligeable	Limitée	**Importante**	Critique
Vraisemblance	**Minime**	~~**Significative**~~	Forte	Maximale

Risque 7 : Risques liés à la disponibilité du catalogue qui doit rester disponible sous 6 heures				
Gravité	Négligeable	**Limitée**	Importante	Critique
Vraisemblance	Minime	Significative	**Forte**	Maximale

Risque 8 : Risques liés à l'intégrité du catalogue pour lequel une corruption doit être détectable				
Gravité	Négligeable	Limitée	**Importante**	Critique
Vraisemblance	**Minime**	Significative	~~**Forte**~~	Maximale

5.1.3 - Établir une déclaration d'applicabilité

Paramètre à prendre en compte	Explication / Justification
Contraintes organisationnel	
Le support client s'effectue uniquement les jours ouvrés	**Non pris en compte** Les horaires du service client n'influent pas sur le site internet.
Une personne de l'équipe IT entièrement dédiée au clients particuliers	**Pris en compte** Il doit y avoir une personne qui s'occupe de la maintenance du site internet.
Deux personnes de l'équipe IT dédiées aux clients professionnels	**Non pris en compte** Cela n'a aucune conséquence sur le site internet.
Une responsable IT + deux ingénieurs polyvalents	**Pris en compte** Il doit y avoir une personne qui s'occupe de la maintenance du site internet dans le cas où la personne de l'équipe IT entièrement dédiée au clients particuliers n'est pas disponible.
Contraintes de temps	
La qualité de service avec les clients professionnels est prioritaire	**Pris en compte** Les mesures de sécurité prises pour le site internet sont mises en place de sorte à ce que celui-ci n'influe pas sur les clients professionnels.
Contraintes de fonctionnelles	
L'intégration avec l'existant	**Pris en compte** On communique entre le serveur ERP et le serveur du site.
Facilité d'utilisation pour les particuliers	**Pris en compte** Les mesures de sécurité mises en place sont transparentes côté client. Le client est protégé par les mesures de sécurité prises par l'entreprise.
Contraintes stratégiques	
Diversification de l'activité afin d'assurer une activité constante en cas de perte de gros clients professionnels	**Pris en compte** L'activité du site internet n'influe pas sur le service avec les clients professionnels.
Forte concurrence existante	**Pris en compte** Des mesures sont prises contre les potentiels attaques / pirates.
Contraintes budgétaires	
L'activité de vente aux particuliers doit être rentable dans les deux années à venir	**Pris en compte** On évite les différentes pénalités qui pourraient coûter de l'argent à l'entreprise.

5.2 – Mettre en œuvre les mesures de sécurité

5.2.1 - Élaborer le plan et suivre la réalisation des mesures de sécurité

Mesure de sécurité	Responsable	Difficulté	Terme
Renforcer les contraintes sur le contrat du prestataire	Direction	Moyenne	Trimestre
Chiffrer les données sensibles	Equipe IT	Moyenne	Année
Signer les données avec une clé privée	Equipe IT	Moyenne	Année
Sécurisation des échanges entre serveur ERP et serveur site	Equipe IT	Difficile	Trimestre
Sauvegarde	Equipe IT	Faible	Trimestre
Changer régulièrement les mots de passe.	Direction	Faible	Année
Organiser une conférence sur la sensibilisation à la sécurité en entreprise.	Direction	Faible	Année

5.2.2 - Prononcer l'homologation de sécurité

Le Directeur de CloseNell a prononcé l'homologation de sécurité du cabinet au vu de l'étude réalisée (délimitation du périmètre, appréciation des risques, élaboration du plan d'action, mise en évidence des risques résiduels...) et des livrables élaborés (note de cadrage, note de stratégie, politique de sécurité de l'information).

Cette homologation de sécurité est valable un an et pourra être renouvelée tous les ans.

La mise en œuvre du plan d'action devra être démontrée, ainsi que l'amélioration continue de l'étude de sécurité.