Institut des
Risques
Industriels,
Assuranciels et
Financiers

APPLICATION DE LA MÉTHODE EBIOS À L'ENTREPRISE OLD RHUM

Étude de cas

MASTER

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Novembre 2006 Version 1.4

SOMMAIRE

ELEFEBVRE@EFFISOFT.com

1 Présentation de la société OLD RHUM

La société OLD RHUM distille, met en bouteilles et distribue du rhum et des apéritifs pour la Grande et Moyenne Distribution et la restauration.
Le rhum est importé des Antilles et vieilli en fut. Plusieurs gammes de rhum sont fabriquées en fonction de la qualité, de l'âge du rhum… OLD RHUM fabrique également des cocktails à base de rhum type planteur ou daïquiri.
Toutes les activités, direction, production et administration sont regroupées sur un site.
OLD RHUM est une société familiale qui emploie 300 personnes.
La société est également propriétaire de distilleries aux Antilles pour lui assurer son approvisionnement en rhum. Le stockage du rhum étant cher et dangereux, la société travaille à flux tendu.

Les activités de la Société OLD RHUM sont réparties dans les services suivants :

Pôles	Services	Nombre de postes

Direction	Direction	7
	Communication	2
Vente	Commercial	15
	Marketing	3
Finance	Comptabilité / Contentieux	7
	Ressources humaines	3
Production	Production	15
	Maintenance / Travaux neufs	4
Services généraux	Informatique	4
	Logistique / Achat	3
	Qualité / Sécurité / Environnement	4
	Recherche et Développement	5
	TOTAL	72

La concurrence étant importante sur ce secteur, le directeur de OLD RHUM a décidé depuis 3 ans d'informatisé lourdement son entreprise et de proposer à ses clients de passer leurs commandes par Internet (mais pas encore de payer). Les relations avec les distilleries aux Antilles se font essentiellement par Internet.

Soucieux de la pérennité de son entreprise, le directeur souhaite réaliser une étude sur la Sécurité du Système d'Information de son entreprise.

L'étude aura pour objectif de sécuriser les éléments constitutifs de l'exploitation de la société Old Rhum. Elle couvre l'analyse des éléments suivants :

Aspects physiques :

Les aspects fonctionnels :

Les informations traitées ;

L'environnement d'exploitation dont l'administration de la sécurité ;

Les échanges et réseau.

Les éléments suivants sont exclus du champ de l'étude :

l'informatique de production.

2 VOTRE MISSION

Vous êtes contactés par la société Old Rhum pour réaliser en relation avec le service informatique une étude sur la Sécurité de son Système d'Information. Vous décidez pour cela d'utiliser la méthode EBIOS.

Vous organisez un Comité de Pilotage avec les directeurs des services concernés pour présenter votre démarche, établir le champ de l'étude et faire valider vos premières réflexions.

A la suite de ce Comité de Pilotage, les éléments suivants ont été validés :

Champ de l'étude :

L'ensemble du système d'information de l'entreprise excepté l'informatique de production

Groupes fonctionnels :

Trois Groupes Fonctionnels ont été constitués :

GF 1 : Direction / Vente
GF 2 : Finance
GF 3 : Production / Services généraux

Échelle de cotation des impacts :

L'échelle de cotation des impacts suivante a été validée :

0 → Pas d'impact
1 → Perturbation, retard de livraison, perte financière faible
2 → Retard important, perte de clientèle faible, impact financier moyen
3 → Difficulté importante, mouvements sociaux, perte financière lourde.
4 → Mise en péril de l'activité

3 RÉUNIONS DES GROUPES FONCTIONNELS

Vos premières réunions avec les groupes fonctionnels vous permettent d'identifier les informations et les applications de l'entreprise ainsi que les serveurs les hébergeant.

	SERVEURS
GF 1 : Direction / Vente	
Informations :	
▪ Fichiers clients	**A**
Applications :	
▪ NET COM : Commandes en ligne	**A**
▪ VENTE Pro : Gestion commerciale	**A**
GF 2 : Finance	
Informations :	
▪ Comptabilité de la société	**B**
▪ Fichiers du personnel	**B**
Applications :	
▪ WINPAI : Salaires	**B**
▪ Compta 500 : Comptabilité	**B**
▪ FACTUR + : Édition des factures	**B**
GF 3 : Production / Services généraux	
Informations :	
▪ Formules des cocktails	**D**
▪ Fichiers fournisseurs	**C**
▪ Produits en développement	**D**
▪ Stocks de matières premières	**C**
▪ Stocks de produits finis	**C**
Applications :	
▪ WIN TRAVO : Planification de la maintenance et des interventions	**C**
▪ STOCK 2000 : Gestion des stocks	**C**
▪ EFFLU + : Gestion des rejets	**C**
▪ OPEN LOG : Gestion de la logistique	**C**

Pour tous les services :	
▪ Intranet	**E**
▪ Extranet	**E**
▪ Bureautique	**-**

4 EXPRESSIONS DES BESOINS

Conformément à la méthode EBIOS, vous devez estimer les besoins en sécurité de chaque information et application.

Dans un premier temps, imaginez les événements significatifs pour chacun des critères : Disponibilité, Intégrité et Confidentialité.

Ensuite, indiquer les types impacts potentiels pertinents pour la société (perte financière, perte de clients…).

Enfin, en utilisant l'échelle de cotation que vous avez fait valider par la direction, fabriquez un tableau pour chaque groupe fonctionnel permettant d 'évaluer l'impact de chaque événement pour chaque application et information en indiquant à chaque fois le type d'impact concernés (voir tableau ci-dessous).

« GF n »	**Application 1**	**Application 2**	**Information 1**	**Information 2**
Disponibilité				
Événement 1				
Événement 2				
Événement 3				
Intégrité				
Événement 1				
Événement 2				
Événement 3				
Confidentialité				
Événement 1				
Événement 2				
Événement 3				

5 RÉUNIONS DU GROUPE TECHNIQUE ET AUDIT DU SITE

La société Old Rhum est implantée au sein d'une zone industrielle, dans trois bâtiments.

Bâtiment 1 : direction et administratif
Bâtiment 2 : production
Bâtiment 3 : stockage et informatique

Les salles informatiques sont situées dans une zone du bâtiment 2. L'accès à cette zone est libre. L'entrée des salles techniques est réservée au personnel habilité, protégée par un digicode.
Les sauvegardes sont placées dans un coffre ignifuge situé dans la zone informatique, dans une armoire située dans un couloir.

Les vulnérabilités suivantes ont été identifiées :

1.	Les locaux ne sont pas équipés de détection incendie
2.	Le magasin contenant des stocks importants de papier, se trouve à proximité des salles informatiques ; des déchets de papier, plus facilement inflammables, s'y trouvent également stockés
3.	Le personnel de la société fournisseur du logiciel a un accès direct aux serveurs
4.	Certaines issues de secours sont difficiles d'accès
5.	On note la présence de papiers et de cartons en salle informatique
6.	Les armoires de climatisation ne sont pas redondantes
7.	L'onduleur est d'un modèle ancien, qui n'est plus maintenu
8.	Les faux planchers ne sont pas équipés de système d'extinction
9.	Il existe des badges qui n'ont pas été désactivés pour des personnes qui ont quitté le site
10.	En ce qui concerne le secret professionnel, le personnel temporaire ne suit pas de formation initiale
11.	Le parc informatique inclut des matériels anciens
12.	Les intervenants extérieurs ne sont pas liés par des engagements individuels de sécurité
13.	La procédure sécuritaire de ré-attribution des mots de passe après blocage peut être mise en défaut

14.	Il est possible de se connecter à distance sur les comptes d'administration
15.	La robustesse des mots de passe (système et application) n'est pas testée
16.	Il n'a pas été diffusé de règles et il n'a pas été effectué de sensibilisation du personnel quant à la séparation des pouvoirs
17.	Certaines compétences informatiques ne sont pas redondantes
18.	Les caméras placées dans certaines salles sont renvoyées sur un écran placé dans la salle de pupitrage, donc sans effet lorsqu'il n'y a pas de personnel présent
19.	Certains postes ont un accès à Internet direct via un modem et peuvent donc recevoir des programmes malveillants (bombe logique, virus, ver)
20.	L'extinction est effectuée par un système sprinkler ; ce système protège les bâtiments et les personnes, mais, en cas de déclenchement, les matériels de la zone concernée seraient gravement endommagés. Il présente également un risque potentiel de dégât des eaux (fuite ou déclenchement intempestif)
21.	De nombreux passages de tuyauteries (avec vannes) sont présents en salle
22.	Le personnel n'est pas formé ni sensibilisé à la gestion des mots de passe
23.	Possibilité d'erreur dans la configuration du Firewall. Aucune procédure d'audit de la configuration n'est réalisée.
24.	Le code d'accès à la salle machine n'a pas été changé depuis longtemps
25.	Certains faux plancher ne sont pas cloisonnés
26.	Le personnel utilise des disquettes pour transférer des données sans que ces procédures ne soient formalisées ou contrôlées.
27.	Les armoires de climatisation ne sont pas équipées de bac de rétention
28.	Certaines entrées d'air ne sont pas filtrées
29.	Le bâtiment n'est pas équipé de protection contre la foudre
30	Aucun équipement n'est secouru sur un groupe électrogène

31.	Certaines portes appartenant à des cloisonnements coupe-feu sont volontairement bloquées en position ouverte
32.	Les extincteurs ne sont pas signalés
33.	Attribution de privilèges non autorisés à des utilisateurs
34.	Aucune consigne spécifique en cas d'incendie n'est affichée ou a été diffusée et les consignes d'évacuation ne sont pas mises à jour
35.	Les mots de passe des comptes d'administration ne sont pas changés régulièrement ; il n'est pas mis en œuvre d'utilitaire pour la vérification des règles de composition et de gestion (longueur, changement périodique)
36.	Certains faux plancher ne sont pas cloisonnés
37.	Les arrivées de lignes ne sont pas protégées à l'extérieur du bâtiment
38.	On fume en salle
39.	Possibilité d'introduire des infections associées aux fichiers reçus
40.	On note la présence de poubelles en salle ; celles-ci ne sont pas anti-feu
41.	Dans les faux plancher, les câbles (télécommunication et électricité) sont mélangés et ne sont pas placés sur des chemins de câble
42.	Les locaux ne sont pas placés sous télésurveillance en dehors des heures de présence
43.	Pas de remontée d'alerte en cas de détection d'anomalie ou d'incident
44.	Les règles de gestion des mots de passe ne sont pas diffusées auprès du personnel
45.	Le réseau de sprinklers parcourt tout le bâtiment
46.	Les armoires de climatisation sont situées en salle ; elles sont alimentées en eau glacée
47	Le local France Télécom est mal protégé

48.	Le contrôle d'accès aux bâtiments est sommaire : l'entrée des personnes n'est pas surveillée par caméra et un portail principal offre un large accès au magasin et de là aux salles techniques. En outre, il existe des accès (non utilisés, mais l'effraction est possible) donnant sur le quai à l'arrière du bâtiment

Cette liste n'est exhaustive, d'autres vulnérabilités peuvent être identifiées grâce aux éléments fournis dans le reste du document.

6 ÉTUDE DES RISQUES

En vous basant sur les différents éléments que vous connaissez (description du site, vulnérabilités…) vous devez, conformément à la méthode EBIOS conduire une étude des risques.

Pour cela, vous effectuerez successivement chacune des taches suivantes :

1. Sélectionner les menaces génériques ;

2. Associer les vulnérabilités spécifiques aux menaces génériques retenues ;

3. Identifier et évaluer les risques spécifiques.

M	V	R	Libellé	D	I	C	T	F/P
M01	V01_01	R01_01	Incendie non maîtrisé dans l'ensemble du bâtiment rendant le siège inutilisable					
M01	V01_01 à V01_0n	R01_02	Incendie non maîtrisé dans la salle informatique - télécommunication rendant le matériel et les installations inutilisables					

7 RECOMMANDATIONS

Pour terminer l'étude, vous devez proposer à la direction des recommandations que vous justifierez en vous appuyant sur les risques identifiés.