

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



Mémoire

Pour l'obtention du diplôme de post graduation spécialisée en
sécurité informatique

Thème :

Elaboration d'une Politique de
Sécurité du Système d'Information
basée sur la méthode EBIOS

Présenté par : Mr KANOUNI Halim

Encadré par :
Mr KHELLADI Lyes

Devant le jury :

Mme S.BENMEZIANE	Présidente
Mme H.BENSEFIA	Examinatrice
Mr D.TANDJAOUI	Examinateur

juin 2007

SOMMAIRE

INTRODUCTION.....	1
CHAPITRE I : SECURITE DE L'INFORMATION ET POLITIQUE DE SECURITE....	10
I.1. INTRODUCTION.....	11
I.2. LA SECURITE DE L'INFORMATION	12
I.2.1 Définition.....	12
I.2.2 La nécessité de la sécurité de l'information	12
I.3. POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION.....	13
I.3.1 Définition de système d'information	13
I.3.2 Définition d'une Politique de Sécurité du Système d'Information.....	13
I.3.3 Nécessité d'une PSSI	14
I.3.4 Démarche d'élaboration d'une PSSI	15
I.3.5 Plan type d'une PSSI	16
I.3.6 Les suites d'une PSSI.....	17
I.4. LA GESTION DES RISQUES	17
I.4.1 Concepts de la gestion des risques	18
I.4.2 Relations entre les concepts de la gestion des risques	19
I.4.3 Nécessité d'un programme de gestion des risques	20
I.4.4 Le processus de gestion des risques.....	20
I.4.5 La gestion des risques en pratique	23
I.4.6 Les référentiels de sécurité.....	23
I.4.6.1 Différence entre norme et méthode.....	23
I.4.6.2 Les normes liées à la gestion des risques	24
I.4.6.2.1 La norme ISO17799	24
I.4.6.2.1.1 Architecture de l'ISO17799 :2000	24
I.4.6.2.1.2 Application de la norme ISO17799.....	24
I.4.6.2.2 La norme ISO15408	25
I.4.6.3 Les méthodes de gestion des risques.....	25
I.4.6.3.1 EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)	25
I.4.6.3.1.1 Démarche	26
I.4.6.3.2 CRAMM (CCTA Risk Analysis and Management Method)	26
I.4.6.3.2.1 Démarche	26
I.4.6.3.3 ITBPM (Information Technology Baseline Protection Manual)	27
I.4.6.3.3.1 Démarche	28
I.4.6.3.4 MEHARI (METHode Harmonisée d'Analyse de Risques)	29
I.4.6.3.4.1 Démarche	29
I.4.6.3.5 OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)	31
I.4.6.3.5.1 Démarche	31
I.4.6.3.6 NIST 800-30	33

I.4.6.3.6.1 Démarche	33
I.4.6.4 Synthèse	36
I.4.6.5 Critères de choix d'une méthode.....	38
I.5. CONCLUSION	40
CHAPITRE II : LA METHODE EBIOS	41
II.1 INTRODUCTION.....	42
II.2 CHOIX DE LA METHODE POUR L'ELABORATION DE LA PSSI.....	42
II.2.1 La méthode EBIOS.....	42
II.2.1.1 Présentation	42
II.2.1.2 Les atouts d'EBIOS.....	42
II.2.1.3 Ce que ne permet pas la méthode EBIOS	45
II.2.2 Le guide PSSI de la méthode EBIOS	46
II.2.2.1 Objectifs	46
II.2.2.2 Champ d'application.....	46
II.2.2.3 Les atouts du guide PSSI.....	46
II.3 LA DEMARCHE DETAILLEE D'EBIOS.....	50
II.3.1 Etude de contexte.....	50
II.3.1.1 Activité 1.1- Etude de l'organisme.....	52
II.3.1.2 Activité 1.2- Etude du système cible	53
II.3.1.3 Activité 1.3- Détermination de la cible de l'étude de sécurité	54
II.3.2 Expression des besoins de sécurité	54
II.3.2.1 Activité 2.1- Réalisation des fiches de besoins	55
II.3.2.2 Activité 2.2- Synthèse des besoins de sécurité	56
II.3.3 Etude des menaces	56
II.3.3.1 Activité 3.1- Etude des origines des menaces.....	57
II.3.3.2 Activité 3.2- Etude des vulnérabilités	58
II.3.3.3 Activité 3.3- Formalisation des menaces.....	59
II.3.4 Identification des objectifs de sécurité	59
II.3.4.1 Activité 4.1- Confrontation des menaces aux besoins.....	60
II.3.4.2 Activité 4.2- Formalisation des objectifs de sécurité.....	61
II.3.4.3 Activité 4.3- Détermination des niveaux de sécurité.....	62
II.3.5 Détermination des exigences de sécurité	62
II.3.5.1 Activité 5.1- Détermination des exigences de sécurité fonctionnelles	63
II.3.5.2 Activité 5.2- Détermination des exigences de sécurité d'assurance.....	64
II.4 UTILISATION DE LA METHODE EBIOS POUR ELABORER UNE PSSI.....	64
II.5 CONCLUSION	70
CHAPITRE III : APPLICATIONS ET RESULTATS.....	71
III.1 INTRODUCTION.....	72

III.2 LES ETAPES DE DEFINITION DE LA PSSI.....	72
III.2.1 Organisation projet	72
III.2.2 Réalisation d'une étude EBIOS globale	72
III.2.3 Définition et sélection des principes de sécurité	74
III.2.4 Elaboration des règles de sécurité.....	74
III.3 ETUDE EBIOS GLOBALE	74
III.3.1 Etude de contexte.....	74
III.3.2 Expression des besoins de sécurité	77
III.3.3 Etude des menaces	80
III.3.4 Identification des objectifs de sécurité	84
III.3.5 Détermination des exigences de sécurité	90
III.4 CONCLUSION	93
CONCLUSION	94
GLOSSAIRE	97
BIBLIOGRAPHIE	106

LISTE DES FIGURES

Fig.I.1 : Relations entre les concepts de gestion des risques	Erreur ! Signet non défini.
Fig.I.2 : Le processus de gestion des risques	Erreur ! Signet non défini.
Fig.I.3 : Approche de la sécurité par ITBPM.....	Erreur ! Signet non défini.
Fig.I.4 : La démarche de MEHARI	Erreur ! Signet non défini.
Fig.I.5 : La conduite d'une analyse des risques selon NIST 800-30	Erreur ! Signet non défini.
Fig.I.6 : La conduite d'une gestion des risques selon NIST 800-30	Erreur ! Signet non défini.
Fig.II.1 : Démarche EBIOS globale	Erreur ! Signet non défini.
Fig.II.2 : Synoptique détaillé de l'étude de contexte	Erreur ! Signet non défini.
Fig.II.3 : Synoptique détaillé de l'expression des besoins de sécurité	Erreur ! Signet non défini.
Fig.II.4 : Synoptique détaillé de l'étude des menaces	Erreur ! Signet non défini.
Fig.II.5 : Synoptique détaillé de l'identification des objectifs de sécurité	Erreur ! Signet non défini.
Fig.II.6 : Synoptique détaillé de la détermination des exigences de sécurité	Erreur ! Signet non défini.
Fig.II.7 : Exploitation des résultats d'EBIOS pour élaborer une PSSI	Erreur ! Signet non défini.

LISTE DES TABLEAUX

Tableau.I.1 : Répartition des référentiels selon l'orientation	Erreur ! Signet non défini.
Tableau.I.2 : Approches des méthodes.....	Erreur ! Signet non défini.