



Table des matières

Avant-propos	3
Chapitre 1. Introduction	9
1.1 Les enjeux de la cybersécurité.....	9
1.2 Une définition de la cybersécurité.....	11
1.3 Principe et plan de cet ouvrage.....	14
Chapitre 2. Systèmes de Management de la Sécurité de l'Information	17
2.1 Justifier les mesures de sécurité.....	17
2.2 Généralités sur les mesures de sécurité.....	21
2.2.1 Mesures et objectifs de sécurité.....	21
2.2.2 Mesures de sécurité techniques et non-techniques.....	23
2.2.3 Des mesures de sécurité au SMSI.....	24
2.3 Contrôle d'accès.....	28
2.4 Journalisation, imputabilité et audit.....	30
2.5 Identification & authentification.....	39
2.6 Sécurisation du réseau.....	44
2.7 Sécurisation des locaux et de l'environnement de travail.....	56
2.8 Mesures de sécurité relatives au personnel.....	60
2.9 Classification et marquage.....	65
2.10 Estimation et traitement des risques.....	68
2.11 Gestion des biens sensibles.....	72
2.12 Résumé.....	77
Chapitre 3. La cybersécurité dans le développement	79
3.1 Notions-clés pour la cybersécurité dans le développement.....	84
3.1.1 Menace.....	85
3.1.2 Vulnérabilités et bugs de sécurité.....	86
3.1.3 Mécanismes de sécurité.....	89
3.1.4 Argumentaires de sécurité.....	90

3.2 Rôles et responsabilités pour la sécurité dans le développement.....	94
3.2.1 Le pôle d'expertise en cybersécurité.....	95
3.2.2 L'expert cybersécurité projet.....	96
3.2.3 L'équipe de développement.....	97
3.3 La cybersécurité à chaque étape du développement.....	98
3.3.1 Études, préparation, démarrage.....	99
3.3.2 Planification, spécification et conception.....	104
3.3.3 Implémentation, vérification et validation.....	110
3.3.4 La sécurité de l'environnement de développement.....	115
3.4 Résumé.....	116
Chapitre 4. Cybersécurité opérationnelle.....	119
4.1 Gestion des identités et des autorisations.....	121
4.2 Maintien en Condition de Sécurité.....	124
4.3 Audits de sécurité périodiques.....	127
4.4 Fin de vie et recyclage.....	131
4.5 Résilience opérationnelle des SI.....	132
4.6 Réponse à incident de sécurité informatique.....	135
4.6.1 Préparation.....	137
4.6.2 Détection & Analyse.....	140
4.6.3 Endiguement, Éradication & Reprise.....	144
4.6.4 Clôture.....	146
4.7 Plan de Secours des Systèmes d'Information.....	150
4.7.1 Préparation.....	150
4.7.2 Détection & analyse.....	155
4.7.3 Reprise.....	158
4.7.4 Clôture.....	162
4.8 Résumé.....	163
Chapitre 5. Cyberattaques, cybercriminalité, cyberguerre.....	165
5.1 Une brève histoire de la SSI / cybersécurité.....	166
5.2 Cyberattaques, cybercriminalité, cyberespionnage.....	172
5.2.1 Les malwares.....	172
5.2.2 La cybercriminalité.....	173
5.2.3 Le cyberespionnage.....	178
5.3 Cyberguerre et cyberdéfense.....	185
5.3.1 Un exemple de cyberattaque étatique : Stuxnet.....	186
5.3.2 Stratégie de cyberdéfense des États.....	190
5.3.3 L'approche française.....	195
5.4 Résumé.....	198
Perspectives et conclusions.....	201
L'informatique en nuage.....	202
Le Big Data.....	206
Les objets communicants.....	210
Conclusion : Penser la cybersécurité.....	212
Liste des abréviations.....	219
Bibliographie.....	223
Index.....	231