

ALEXANDRE FERNANDEZ-TORO



Sécurité opérationnelle

2^e édition

Conseils pratiques pour sécuriser le SI

— **EYROLLES** —

Table des matières

Avant-propos	1
À qui s'adresse cet ouvrage?	1
Structure de l'ouvrage	1
Remerciements	2
 Partie I – Aspects concrets de la sécurité opérationnelle	
Chapitre 1 – Les différents niveaux de sécurité	5
Connaître le niveau de sécurité réel	5
Différents niveaux de sécurité	6
Quels chantiers lancer?	11
Chapitre 2 – La sécurité des réseaux	15
Cartographier le réseau	15
Sécuriser le réseau	17
Chapitre 3 – Accès distants	23
Enjeux des accès distants	23
À chaque usage sa solution technique	24
Aspects organisationnels	27
Chapitre 4 – Journalisation	33
Usages de la journalisation	33
La problématique de la journalisation	34
Centralisation des journaux	36
Que surveiller?	38
Principaux fournisseurs de journaux	40
Comment traiter les journaux?	41
Chapitre 5 – Mots de passe	47
Différents types de comptes	47

Qualité des mots de passe	50
Gestion des mots de passe	53
Idées reçues sur les mots de passe	55
Chapitre 6 – Sécurité du poste de travail	57
Mesures incontournables	57
Mesures souhaitables	63
Cas particuliers	64
Agir au niveau du master	66
Sécuriser le poste de travail a-t-il encore un sens?	66
Chapitre 7 – Antivirus	69
Pourquoi parler encore d'antivirus de nos jours?	69
Limites des antivirus et solutions	70
Atouts des antivirus	74
Chapitre 8 – Sécurité des services	77
Freins à la sécurité des services	77
Principes de base	78
Sécuriser les serveurs	79
Chapitre 9 – Sauvegardes et restaurations	85
En quoi le RSI peut-il être utile pour les sauvegardes?	85
Cartographier les sauvegardes	86
Restaurations	89
Chapitre 10 – Maîtriser les identités et les accès	93
Complexité de la gestion des identités	93
Approches pour gérer cette complexité	95
Différents points à contrôler	100
Contrôle complémentaire : l'accès aux salles machines	105
Chapitre 11 – Rôle du RSI dans la continuité et la reprise d'activité ..	107
Questions préalables	107
Dispositions de continuité et de reprise	108
Rôle du RSI en temps de paix	109
Rôle du RSI en temps de guerre	116

Chapitre 12 – Gestion des tiers sensibles	119
Qu’entendons-nous par tiers sensible?	119
Principaux points d’attention	121
Chapitre 13 – Gestion des incidents de sécurité	133
Nécessité d’un processus de gestion des incidents	133
Points clés d’un processus de gestion d’incidents	134
Chapitre 14 – Le RSSI face au juridique	141
Enjeux juridiques	141
Bases documentaires incontournables	142
Quelques points sensibles	148
Chapitre 15 – Lutter contre les infrastructures spontanées	153
Qu’entendons-nous par infrastructure spontanée?	153
Une entorse à l’urbanisation des SI	154
Comment éradiquer les infrastructures spontanées	158
Un autre type d’infrastructure spontanée	162
Chapitre 16 – Gérer les expirations bloquantes	163
Certificats	163
Noms de domaines	168
Licences	170
Comment éviter les expirations bloquantes?	171
Pourquoi la gestion des expirations bloquantes relève-t-elle de la sécurité?	173
Chapitre 17 – Sensibilisation	175
Importance de la sensibilisation	175
Différents niveaux de sensibilisation	176
En complément à la sensibilisation	180
Chapitre 18 – Gérer les audits	183
L’importance des audits	183
Comment recevoir les auditeurs	186
Pour faciliter les audits	190
Chapitre 19 – Gérer le tout-venant	193
Généralités	193

Différents types de demandes	194
Traitement des demandes	195
Chapitre 20 – Sécurité industrielle	199
Contexte	199
Lancer une première vague d’actions	201
Mettre à jour les systèmes	202
Limitier les échanges entre les deux mondes	208
Durcir les services restant ouverts sur l’informatique de gestion	211
 Partie II – Compléments sur la sécurité des SI modernes	
Chapitre 21 – La nouvelle donne de la sécurité	217
Nouveaux défis pour les entreprises	217
Les SI en support de ces projets d’entreprise	220
Questions sur la sécurité opérationnelle	223
Chapitre 22 – Le cloud	225
Conséquences du cloud pour la sécurité	225
Sécuriser le cloud spontané	227
Sécuriser le petit cloud	229
Sécuriser le grand cloud	231
Principales mesures de sécurisation	234
Maîtriser les comptes génériques	236
Les CASB	239
Chapitre 23 – Aspects concrets du WebSSO	247
Introduction	247
Usages du WebSSO	250
Problèmes concrets	253
Conclusion	260
Chapitre 24 – Sécuriser les systèmes d’intermédiation	261
Généralités sur les systèmes d’intermédiation	261
Mesures générales de sécurisation	265
Focus sur les services web et les ESB	267
Focus sur les autres systèmes d’intermédiation	273

Chapitre 25 – Le big data	275
Différents types d'utilisation	275
Apports du big data pour la sécurité opérationnelle	277
Limites et risques liés au big data	280
Chapitre 26 – Obstacles à la sécurité opérationnelle	283
Freins à la sécurisation du SI	283
Un besoin flagrant	288
 Partie III – Intégration dans la norme ISO 27001	
Chapitre 27 – La norme ISO 27001	291
Multiplicité des référentiels	291
Les systèmes de management	292
Présentation de la norme ISO 27001	293
Conclusion	297
Chapitre 28 – La norme ISO 27002	299
Présentation	299
Utilisations de la norme	300
Présentation de la norme ISO 27002	301
Chapitre 29 – Intégration de la sécurité opérationnelle à l'ISO 27001	309
Carences des normes ISO	309
Risques liés à la sécurité opérationnelle	310
Ce qu'apporte l'ISO 27001 à la sécurité opérationnelle	312
Processus complémentaires	313
Chapitre 30 – Surveillance du SI et tableaux de bord sécurité	319
Une forteresse sans sentinelles	319
Outils techniques de surveillance	320
Tableaux de bord	324
Chapitre 31 – Sort-on vraiment un jour de la zone d'humiliation?	329
Les méthodes pour sortir de la zone d'humiliation	329
Quelle est la place du RSSI?	332

Annexe 5 – Procédure de gestion des tiers sensibles pour le SI	355
1 – Définition d'un tiers sensible pour le SI	355
2 – Processus	355
Annexe 6 – Règles à respecter par les tiers	357
1 – Introduction	357
2 – Exigences applicables à tous les tiers	357
3 – Exigences applicables aux intégrateurs	358
4 – Exigences applicables aux tiers fournissant des solutions en mode SaaS	358
5 – Exigences applicables aux tiers offrant des services de développement logiciel	359
Annexe 7 – Fiches de sécurité du SI pour les tiers	361
Annexe 8 – Procédure de vue générale des droits	365
1 – Différents domaines concernés	365
2 – Processus général pour chaque domaine	366
3 – Structure du rapport	366
4 – Divers	367
Annexe 9 – Politique des mots de passe	369
1 – Champ d'application	369
2 – Mots de passe applicatifs	369
3 – Mots de passe des infrastructures techniques	370
4 – Contrôle de qualité des mots de passe	371
Annexe 10 – Procédure de gestion des pare-feu	373
1 – Principes généraux	373
2 – Création et modification de règles	373
Annexe 11 – Procédure de gestion des correctifs de sécurité	375
1 – Gestion des correctifs de sécurité	375
2 – Postes de travail	375
3 – Serveurs Windows installés avant le master V512	376
4 – Serveurs Windows installés à partir du master V512 et suivants ...	376
5 – Correctifs urgents	376
6 – Responsabilités	377

Annexe 12 – Procédure de gestion des antivirus	379
1 – Sur les postes de travail	379
2 – Sur les serveurs	379
3 – Alertes virales	380
4 – Exploitation	380
5 – Attaques virales	380
Annexe 13 – Procédure de gestion des journaux	381
1 – Différents journaux	381
2 – Journaux du proxy HTTP sortant	381
3 – Journaux du pare-feu	382
4 – Journaux applicatifs	383
5 – Journaux système	383
Annexe 14 – Procédure de gestion des accès distants	385
1 – Différents types d'accès distant	385
2 – Les liaisons VPN site à site	385
3 – Liaisons VPN d'administration	386
4 – Portail de publication des accès distants	387
5 – APN privée	387
Annexe 15 – Procédure de gestion des incidents de sécurité	389
1 – Processus général	389
2 – Veille	389
3 – Détection	390
4 – Mesures d'urgence	390
5 – Analyse et traitement	391
6 – Alerte sécurité	391
7 – Bilan	392
Annexe 16 – Fiche d'incident 1	393
Annexe 17 – Fiche d'incident 2	395
Annexe 18 – Fiche réflexe 1. Conduite à tenir en cas d'attaque virale ..	397
1 – Grandes étapes	397
2 – Compréhension technique de l'attaque	397
3 – Évaluation de l'impact	398

4 – Contention et éradication.....	398
5 – Rôles et responsabilités	399
Annexe 19 – Fiche réflexe 2. Conduite à tenir en cas d'attaque par hameçonnage	401
1 – Vérification.....	401
2 – En cas d'hameçonnage avéré	401
3 – Rôles et responsabilités	402
Annexe 20 – Plan de secours informatique.....	403
1 – Définitions	403
2 – Généralités.....	403
3 – Plan de secours, hors situation d'urgence	403
4 – Plan de secours, en situation d'urgence	406
5 – Responsabilités.....	406
Annexe 21 – Plan de contrôle sécurité.....	409
Fiche « charte utilisateur ».....	410
Fiche « appréciation des risques »	411
Fiche « sensibilisation à la sécurité du SI »	412
Fiche « sauvegardes et restaurations ».....	413
Fiche « communications avec les tiers »	414
Fiche « plan de secours informatique »	416
Index.....	417