

Sécurité Internet

Stratégies et technologies

Solange Gheraouti-Hélie

INFORMATIQUES

DUNOD



-005-136-1

2-005-136-1

Sécurité Internet

Stratégies et technologies

Solange Chernaouti-Hélie

*Professeur d'informatique à l'École des Hautes Études Commerciales (HEC)
de l'université de Lausanne*

DUNOD

Table des matières

Chapitre 1 – De l'innovation technologique à la sécurité informatique	1
1.1 La révolution informationnelle	1
1.1.1 Numérisation et technologies numériques	1
1.1.2 Innover pour évoluer	2
1.1.3 Impacts	3
1.2 Conséquences pour les entreprises	3
1.2.1 Reconsidérer les échanges	3
1.2.2 Le risque technologique	4
1.3 Des nouvelles pratiques à l'info-exclusion	5
1.3.1 Évolution des usages	5
1.3.2 Les technologies : facteur de distinction ou de discrimination sociale ?	6
1.3.3 Accompagner la révolution informationnelle	6
1.4 Conclusion	7
Chapitre 2 – Les télécommunications à l'heure d'Internet	9
2.1 Mise en perspective historique du monde des télécommunications	9
2.2 Caractéristiques et éléments constitutifs des réseaux de télécommunication	11
2.2.1 Supports d'interconnexion	13
2.2.2 Éléments de connectique	13
2.2.3 Machines spécialisées et serveurs d'information	14
2.2.4 Aspects logiciels	14
2.3 Infrastructure de télécommunication et autoroute de l'information	15
2.4 Le réseau Internet	15
2.4.1 L'infrastructure Internet	15
2.4.2 Les services de l'Internet	17
2.5 Conclusion	18

Chapitre 3 – Les nouveaux paradigmes du cyberspace	19
3.1 Intranet, extranet et réseaux privés virtuels	19
3.1.1 Des opportunités organisationnelle et technologique	19
3.1.2 Une nouvelle organisation du travail	21
3.1.3 Du client-serveur à l'intranet	21
3.1.4 Des avantages pour l'entreprise	22
3.1.5 Des compétences managériales spécifiques	24
3.2 Le Web au-delà de la technique	24
3.2.1 Cyberbusiness, l'indispensable dimension marketing	25
3.2.2 Les conditions de succès d'un projet Internet	26
3.2.3 Le commerce électronique	29
3.3 Conclusion	30
Chapitre 4 – La criminalité dans le cyberspace	31
4.1 Nouvelles technologies et criminalité	31
4.1.1 Organisations criminelles	32
4.1.2 Les menaces émergentes	34
4.1.3 Le cyberdélinquant	36
4.2 Internet face à l'éthique	38
4.2.1 Éthique ou éthiques ?	38
4.2.2 À réseau global, éthique globale ?	39
4.2.3 Internet et liberté d'expression ?	39
4.2.4 Internet, l'insaisissable ?	40
4.2.5 (In)suffisances de l'auto-contrôle ?	41
4.2.6 Qualité de l'information ?	42
4.2.7 Vers une déontologie de l'Internet commercial ?	43
4.3 Conclusion	43
Chapitre 5 – Périmètre de la sécurité informatique	45
5.1 Principe premier de la sécurité informatique	45
5.2 Systèmes informatiques et sécurité	46
5.2.1 Capacités déterminantes d'un système	46
5.2.2 De la capacité d'un système aux critères de sécurité	47
5.2.3 Une nécessaire éthique	48
5.3 La technique ne suffit pas	49
5.3.1 Une gestion rigoureuse	49
5.3.2 Architecture de sécurité et approche systémique	51

5.4 Domaines d'application de la sécurité	53
5.4.1 Sécurité physique	54
5.4.2 Sécurité de l'exploitation	55
5.4.3 Sécurité logique	56
5.4.4 Sécurité applicative	57
5.4.5 Sécurité des télécommunications	58
5.5 Conclusion	59
 Chapitre 6 – Stratégie et politique de sécurité	61
6.1 Des besoins réels et des propriétés à satisfaire	61
6.1.1 Objectif central de la sécurité	61
6.1.2 La mission de sécurité informatique	64
6.1.3 Conditions de succès d'une démarche sécurité	64
6.2 Mise en place de la sécurité	67
6.3 Maîtriser les risques	68
6.4 Déterminer une politique de sécurité	69
6.4.1 Définir une stratégie sécuritaire	69
6.4.2 Des questions simples, des réponses précises	71
6.4.3 Réaliser une politique de sécurité	71
6.4.4 Les mesures de la sécurité	72
6.4.5 Se protéger et réagir aux intrusions	74
6.4.6 Spécifier un plan de secours	76
6.5 Quelques constats	79
6.6 Conclusion	80
 Chapitre 7 – Gérer la sécurité	81
7.1 Utiliser une démarche méthodologique	81
7.1.1 De la stratégie de sécurité à sa réalisation	83
7.1.2 Minimiser le coût de la sécurité	84
7.1.3 Utiliser les critères d'évaluation de la sécurité	85
7.1.4 Assurer le risque	86
7.1.5 Effectuer une veille technologique de la sécurité	87
7.2 Organisation structurelle de la sécurité	88
7.2.1 Le comité de direction	88
7.2.2 Le service de sécurité	89
7.2.3 L'organe de révision	89
7.2.4 Les acteurs	90

7.3 Aspects contractuel et juridique	91
7.4 Conclusion	94
Chapitre 8 – Auditer les systèmes d'information et leur sécurité	95
8.1 Contexte d'application de l'audit de la sécurité	95
8.2 Le référentiel de l'audit : la politique de sécurité	96
8.3 Audit, auditeur et organe de révision	97
8.3.1 Rôle de l'auditeur	97
8.3.2 Différents types d'audit	97
8.3.3 Contrôle de gestion informatique	100
8.3.4 Contrôle interne opérationnel informatique	104
8.3.5 Audit informatique	106
8.3.6 Audit, qualité et certification ISO 9000	113
8.4 Conclusion	114
Chapitre 9 – Les technologies de la sécurité	117
9.1 Mettre en œuvre la sécurité	117
9.1.1 De la sensibilité des données à leur protection	117
9.1.2 Entre pertinence et performance : à la recherche d'un optimum	119
9.2 Réaliser confidentialité et authentification	119
9.2.1 Systèmes de chiffrement	120
9.2.2 Quelques aspect légaux relatifs au chiffrement	125
9.2.3 Enveloppe digitale	127
9.2.4 Assurer l'authentification par la certification	128
9.2.5 Assurer la non-répudiation par un tiers de confiance	129
9.2.6 Assurer l'authentification par signature digitale	130
9.3 Intégrité des données	131
9.3.1 Constat	131
9.3.2 Assurer l'intégrité par une empreinte digitale	131
9.3.3 Assurer l'intégrité en se protégeant des virus	132
9.4 Assurer la disponibilité des ressources	135
9.4.1 Importance du dimensionnement	135
9.4.2 Gestion des sauvegardes	135
9.4.3 Gestion des comptes des utilisateurs	135
9.4.4 Gestion des groupes d'utilisateurs	136
9.5 Conclusion	136

Chapitre 10 – Mise en œuvre de la sécurité en télécommunication	137
10.1 L'accès sécurisé aux ressources informatiques	137
10.1.1 Le contrôle d'accès	137
10.1.2 Utilisation des certificats pour contrôler l'accès à un serveur Web	139
10.1.3 Démarche de mise en place d'une solution de gestion sécurisée des accès	142
10.1.4 Gestion des autorisations d'accès basée sur l'usage d'un serveur de noms	142
10.2 Mise en œuvre de la sécurité lors du transfert de données	143
10.2.1 Problématique générale	143
10.2.2 La sécurité au niveau du routage	144
10.2.3 La sécurité au niveau des serveurs de noms	146
10.2.4 La sécurité en X.25	147
10.2.5 La sécurité en Frame Relay	148
10.2.6 La sécurité avec les hauts débits	149
10.2.7 La sécurité avec IP	158
10.3 Protéger les communications	159
10.3.1 Protection de l'infrastructure de support	159
10.3.2 Protection du réseau de transport	160
10.3.3 Protection au niveau de l'utilisateur	161
10.3.4 Constat	161
10.3.5 Polémique : sécuriser l'infrastructure versus sécuriser l'application ?	162
10.4 Risques liés à des tiers lors de la mise en œuvre des communications	164
10.5 Conclusion	164
Chapitre 11 – Menaces et attaques via Internet	165
11.1 Problèmes sécuritaires de l'infrastructure Internet	165
11.1.1 Historique	165
11.1.2 Le protocole Internet	166
11.1.3 L'infrastructure Internet	168
11.2 Attaques via Internet	169
11.2.1 L'usurpation de mots de passe	169
11.2.2 Accès au fichier de mots de passe	172
11.2.3 Techniques de pénétration fondées sur le leurre	174
11.2.4 Attaque par inondation de messages	180
11.2.5 Attaque par buffer overflow	181

11.3 Développer une stratégie de reconnaissance des attaques	182
11.3.1 Stratégie préventive	182
11.3.2 Stratégie réactive	183
11.4 Conclusion	184
Chapitre 12 – La sécurité des applications Internet	185
12.1 La messagerie électronique	185
12.1.1 Le contexte de la messagerie	185
12.1.2 Problème sécuritaire	187
12.1.3 Recommandations	187
12.1.4 S/MIME	188
12.1.5 PGP	189
12.1.6 Quelques recommandations pour sécuriser le serveur de messagerie et le poste de l'utilisateur	191
12.2 Sécuriser un serveur de noms DNS	192
12.2.1 Rôles	192
12.2.2 Domaine de nommage	192
12.2.3 Recommandations	194
12.3 Mécanismes de sécurité pour les applications Internet	194
12.3.1 Secure Sockets Layer (SSL)	194
12.3.2 Secure HTTP (S-HTTP)	195
12.4 Authentification des applications	195
12.4.1 Kerberos	195
12.4.2 Le service d'authentification X.509	196
12.5 Conclusion	197
Chapitre 13 – Le protocole IP sécurisé : IPSec	199
13.1 Prise en compte des impératifs de sécurité au niveau du protocole IP	199
13.2 La version 6 du protocole Internet : IPv6 (IPnG)	200
13.2.1 Spécificités d'IPv6	200
13.2.2 Constat	201
13.3 Protocole Internet sécurisé (IPSec)	201
13.3.1 Présentation générale	201
13.3.2 Services IPSec et association de sécurité	202
13.3.3 Implantation IPSec	203
13.3.4 Modes opératoires	204

13.3.5 L'extension d'authentification (AH)	205
13.3.6 L'extension de confidentialité-authentification (ESP)	205
13.3.7 Gestion des clés	206
13.3.8 Remarque	207
13.4 Créer des réseaux privés virtuels avec IPSec	207
13.5 Conclusion	208
Chapitre 14 – La sécurité des intranets : les firewalls	209
14.1 Intranet et sécurité	209
14.1.1 La notion d'intranet	209
14.1.2 Constat d'architecture	211
14.1.3 Principes de sécurité d'un intranet	211
14.2 Les firewalls : éléments de la sécurité	212
14.2.1 Caractéristiques d'un firewall	212
14.2.2 Le cloisonnement d'un réseau	213
14.2.3 Différents types de firewalls et d'architectures	214
14.2.4 Choix d'un firewall	218
14.2.5 Recommandations	219
14.3 Serveur Web et firewall	219
14.4 Recommandations pour renforcer la sécurité d'un serveur Web	220
14.4.1 Renforcer la sécurité du système d'exploitation	221
14.4.2 Surveiller les demandes de connexion	221
14.4.3 Utiliser des scripts CGI sécurisés	221
14.4.4 Se méfier des applets téléchargeables	222
14.4.5 Se méfier des browsers Web, des serveurs caches et des moteurs de recherche	224
14.4.6 Administration et exploitation de qualité d'un serveur Web	224
14.5 Conclusion	224
Chapitre 15 – Sécurité du commerce électronique	227
15.1 Le commerce électronique sur Internet	227
15.2 Dimension multidisciplinaire des solutions de sécurité	228
15.3 Sécuriser les transactions commerciales	229
15.3.1 Sécuriser la connexion entre l'acheteur et le vendeur	229
15.3.2 Sécuriser le serveur	230
15.4 Notions de confiance et de contrat dans le monde virtuel	231
15.5 Conclusion	232

Chapitre 16 – La sécurité par la gestion de réseaux	233
16.1 Le contexte de la gestion de réseau	233
16.1.1 Augmenter les performances de l'entreprise	233
16.1.2 Acteurs du réseau et besoins	234
16.1.3 Activités de gestion	236
16.2 Planification stratégique	236
16.2.1 Schéma directeur télécoms	237
16.2.2 Conception de réseau	242
16.2.3 Modélisation et simulation	244
16.2.4 L'assurance qualité	246
16.3 Assurer la sécurité par la gestion du réseau	247
16.4 La gestion de réseau	249
16.4.1 Principes de gestion	249
16.4.2 Politique de gestion de réseau	250
16.4.3 Fonctions à couvrir	251
16.4.4 Mise en place d'une politique de gestion de réseau	252
16.5 Infogérance	252
16.5.1 Principes de base	252
16.5.2 Gestion des acteurs externes	254
16.6 Conclusion	254
Chapitre 17 – Gestion opérationnelle et sécurité	255
17.1 Mettre en œuvre la stratégie de gestion et assurer performances et sécurité	255
17.1.1 Gestion du parc informatique	256
17.1.2 Gestion tactique	258
17.1.3 Gestion de la qualité de service réseau	259
17.1.4 Gestion comptable et facturation	261
17.1.5 Ingénierie	262
17.1.6 Gestion de la sécurité	263
17.2 Gestion opérationnelle d'un réseau	264
17.2.1 Faire vivre le réseau	264
17.2.2 Gestion des configurations	264
17.2.3 Surveillance et optimisation	265
17.2.4 Maintenance	266
17.2.5 Exploitation	267
17.2.6 Supervision	268
17.2.7 La documentation	269

17.3 Gestion de réseau et SNMP	269
17.3.1 Protocole SNMP et objet de gestion	269
17.3.2 Enregistrement des objets de gestion	271
17.4 Conclusion	273
Références	275
Bibliographie	275
Webographie	276
Quelques adresses	278
Lexique sécurité	279
Index	283