

LA FONCTION RSSI

Guide des pratiques
et retours d'expérience



Bernard Foray

DUNOD

Avant-propos

*« L'expérience, ce n'est pas ce qui arrive à quelqu'un,
c'est ce que quelqu'un fait avec ce qui lui arrive. »*
Aldous Huxley

La sécurité informatique est-elle taboue ? Peut-on en parler aussi librement que d'autres métiers de l'informatique ? Le vieux slogan « pour vivre heureux vivons cachés » s'applique-t-il aussi à la sécurité ? Doit-on continuer à vivre dans une culture du secret ?

Voici quelques-unes des questions auxquelles ce livre est censé apporter des réponses !

Ce livre est une invitation à parcourir ensemble quelques expériences de terrain rassemblées par l'auteur. Il ne faudra y voir aucune révélation sensationnelle sur les modes de protection des entreprises, mais simplement une envie de partager un savoir-faire, une expérience dans l'espoir (secret) de l'enrichir à nouveau. Parler simplement de la sécurité et de la protection des biens de l'entreprise, telle sera l'ambition de cet ouvrage. En parler, tout en faisant quelques réserves lorsque cela s'avérera nécessaire, mais s'ouvrir sur l'extérieur en dévoilant des méthodes, des façons de procéder, des pratiques et exposer clairement le bilan que l'on en tire, c'est le pari qui sera tenu.

La sécurité n'est qu'une histoire de temps : combien de temps doit résister une porte blindée ? *Le temps de décourager un voleur !* Ces simples phrases évoquent à elles seules toute la complexité de la mise en œuvre de mesures de protection, de défense et de correction. Empêcher qui que ce soit de pénétrer chez vous est illusoire. Tout le monde sait que « la sécurité à 100 %, c'est impossible ». Un des objectifs de la sécurité est de dissuader les intrus pour qu'ils passent leur chemin.

Dans tous les cas, il y aura toujours un individu qui saura comment contourner une protection qui semble absolue. Même si cela ne reste que des aventures romancées, des films comme *Ocean Eleven* ou *Haute Voltige* sont là pour nous rappeler

qu'avec quelques moyens, certes sophistiqués, et un plan bien élaboré, des personnes mal intentionnées arrivent à leurs fins.

Ne voyez dans ces propos aucun désespoir, ne croyez pas qu'être acteur de la sécurité conduit inmanquablement à être désabusé. Bien au contraire, cela doit nous inciter à être encore plus performant en mettant en œuvre des contre-mesures préventives et de détection. Il faut se servir de toutes ses expériences pour apporter des corrections et des améliorations dans le processus de sécurité, ses implémentations techniques et son organisation. Il ne faudra pas oublier que l'être humain avec ses forces et ses faiblesses est au centre de la sécurité. Il doit être « éduqué » pour devenir vigilant, s'adapter aux situations, se poser les bonnes questions devant des événements même banals pour devenir un vrai acteur de la sécurité, un « *key player* » comme pourraient dire les Anglo-Saxons, un relais des personnes en charge de la sécurité des systèmes d'information.

Les RSSI sont ces personnes. Ce métier est à géométrie variable, englobant parfois la sécurité physique, centré uniquement sur des domaines techniques ou encore prenant en compte les aspects juridiques, la propriété intellectuelle ou le respect de la vie privée au sein de l'entreprise. Il n'y a pas de cycle d'étude, de diplôme de RSSI. On peut être RSSI par hasard, par conviction, par curiosité ou parce que notre sensibilité et la façon dont elle est perçue par les autres nous a naturellement conduit vers ce poste. Nos qualités de communicant sont essentielles dans ce métier. Elles nous placeront dans un rôle où personne ne se demandera ce que l'on y fait. Il apparaîtra comme une évidence que le RSSI contribue à apporter de la valeur à tous ceux qu'ils côtoient, dans et hors de son entreprise.

Pour ceux qui pratiquent cette profession depuis peu ou depuis longtemps, cet ouvrage vous permettra de vous positionner, de vous « étalonner » et de définir sur quelle échelle de valeur vous vous trouvez.

Ce livre ne sera pas centré sur la technique ou les technologies. Ces dernières seront utilisées comme support pour expliquer le socle sur lequel reposent l'organisation et le comportement des acteurs de la sécurité du système d'information.

À qui s'adresse ce livre ?

- aux DSI et RSSI souhaitant trouver des réponses pour leurs problématiques opérationnelles et leur communication sur ce sujet sensible ;
- aux ingénieurs sécurité désireux de savoir dans quel contexte organisationnel et comportemental les produits techniques doivent être implémentés ;
- aux exploitants sécurité pour les aider à communiquer sur la valeur des contre-mesures mise en œuvre pour s'opposer aux menaces ;
- aux PME/PMI qui utiliseront les morceaux choisis du livre pour alimenter leur réflexion sur la gestion de leur risque informatique ;
- aux responsables marketing et ventes, soucieux de connaître et d'appréhender le quotidien des RSSI afin de cibler leur discours ;

- à tous ceux qui revendiquent une appartenance à la communauté sécurité intéressés par la qualification de leur propre expérience.

À l'attention des lecteurs...

Même lorsque cela n'est pas précisé, les exemples et valeurs des figures de l'ouvrage sont fictives. Elles ne correspondent à aucune réalité ni mesure véritable.

Remerciements

Je tiens à remercier toutes les personnes qui ont fait que ce livre ait pu exister tant par l'expérience commune que nous avons vécue que par leur enthousiasme. Ils ont tous croisé ma vie professionnelle en m'apportant ce qu'il me fallait au moment où il me le fallait. J'ai partagé avec eux une vision de la sécurité et une façon de la mettre en œuvre tant sur le plan technique, que comportemental ou encore organisationnel :

- **Marie Barel** pour son apport juridique conséquent dans le chapitre relatif à la charte individuelle relative à la sécurité et pour le plaisir que j'ai eu à déployer conjointement cette charte.
- **Gilles Morieux** pour son savoir-faire en matière de configuration sécurité des systèmes d'exploitation et pour son apport dans la mise en œuvre des politiques techniques de sécurité.
- **Régis Pontier** pour la lutte commune que nous avons eu face aux messages indésirables (et aussi un peu pour les échanges d'adresses de restaurants...).
- **Anthony Der-Krikorian** pour sa passion et l'énergie qu'il a consacrée aux services autour de la PKI.
- **Thierry Evangelista** qui m'a donné l'envie de franchir le pas et d'écrire ce livre et pour son savoir-faire en matière de détection d'intrusion.
- **Yves Ayel** pour sa capacité à prendre en charge la sécurité au sein de la production informatique et la mise en perspective des idées.
- **Aurélien Cabezon** pour m'avoir donné l'occasion d'écrire des articles sur son portail de la sécurité informatique et partagé l'envie de vulgariser la sécurité.
- **Sébastien Desse, Cédric Messeguer, Jean-Yves Oberlé** pour avoir réussi, par leur complémentarité à fonder avec moi un groupe d'utilisateurs sécurité sur la région PACA.
- **Les membres du GREPSSI** (Groupe de réflexion et d'échange sur les problématiques liées à la sécurité des systèmes d'information) pour leur réflexion sur la sécurité et la mobilité et les IDS.
- **Arnaud Gut** avec qui j'ai partagé de multiples aventures dans le domaine des réseaux et des télécommunications.
- **Nicolas Girardin** qui par sa curiosité, la simplicité et le bon sens de ses questions m'a conduit à propager plus largement un savoir-faire.

- **Jean-Paul Carray, Christian Gury** qui ont été mes managers et ont contribué à construire ma vie professionnelle.
- **Thierry Kauffmann** juste parce que c'est le genre de personne que l'on ne rencontre qu'une fois dans son expérience professionnelle.

Enfin et surtout, je remercie **Régine** mon épouse et mes trois enfants **Chloé, Aurélien** et **Léa** pour la patience d'ange qu'ils ont eu pendant que j'écrivais ce livre.

Table des matières

Avant-propos	xiii
------------------------	------

Première partie – La préparation

Chapitre 1 – Processus sécurité et indicateurs de performance.	3
1.1 Assurer la sécurité	4
1.1.1 <i>Manager</i>	4
1.1.2 <i>Opérer</i>	6
1.2 Entrées du processus	9
1.3 Sorties du processus	10
1.4 Points critiques du processus	11
1.5 Vue globale du processus	11
1.6 Indicateurs de mesures (KPI)	12
Chapitre 2 – Missions d'un RSSI	17
2.1 Le blues du RSSI...	17
2.2 ...Et sa valeur ajoutée	18
2.3 La stratégie du gagnant-gagnant	19
2.4 Formalisation des rôles et missions	20
2.4.1 <i>Cadre général</i>	20
2.4.2 <i>Cadre individuel</i>	21
2.4.3 <i>Le mandat du RSSI</i>	23

Chapitre 3 – La roadmap sécurité	25
3.1 À quoi sert une roadmap ?	25
3.2 Le RSSI comme fédérateur.	26
3.3 Quel périmètre ?	26
3.4 Plan d'action	27
3.4.1 Volet stratégique	27
3.4.2 Volet opérationnel – Mise en œuvre	29
3.4.3 Volet exploitation.	31
3.5 Quels moyens.	33
3.5.1 Les moyens humains	33
3.5.2 Le budget.	34
3.6 Échanges	34
3.6.1 Les échanges internes.	34
3.6.2 Les échanges externes.	34
3.7 Échéances.	35
3.8 Un schéma synthétique de la feuille de route.	37
Chapitre 4 – Charte individuelle relative à la sécurité	39
4.1 L'environnement de travail a évolué	39
4.2 Principes juridiques et méthodologiques.	40
4.2.1 Cadre réglementaire	41
4.2.2 La charte est une démarche participative et négociée	43
4.2.3 Information et sensibilisation : le marketing de la sécurité.	44
4.3 La charte de sécurité à l'épreuve de la pratique.	45
4.3.1 Contenu pour le contrôle des communications électroniques	46
4.3.2 Politique de détection et mesure d'efficacité de la charte.	47
4.3.3 Politique d'archivage des traces	50
4.3.4 Conditions d'utilisation des données de surveillance.	51
Chapitre 5 – Externalisation des services IT	55
5.1 Acteurs des projets d'externalisation	56
5.1.1 Outsourcing oui, mais dans quelles limites ?	56
5.1.2 Démarrage du projet	56
5.2 Cadrage du projet d'externalisation	57
5.3 Sélection du fournisseur	58
5.4 Fin de contrat	59
5.5 Canevas de cahier des charges.	60

5.5.1	<i>Exigences générales</i>	60
5.5.2	<i>Exigences détaillées</i>	61
5.5.3	<i>Niveau de service attendu</i>	61

Deuxième partie – Les fondamentaux

Chapitre 6 – Politique de filtrage des pare-feu	65
6.1 Fonctions du pare-feu	65
6.2 Trafic et type de services	66
6.3 Politique générale	67
6.4 Procédures opérationnelles	69
6.4.1 <i>Sécurité physique</i>	69
6.4.2 <i>Stratégie de redondance</i>	70
6.4.3 <i>Changement des règles du pare-feu</i>	70
6.4.4 <i>Enregistrements</i>	71
6.4.5 <i>Administration et maintenance</i>	71
6.4.6 <i>Contrôles et audits</i>	73
6.4.7 <i>Expertise des administrateurs du pare-feu</i>	73
Chapitre 7 – Politiques techniques de sécurité.	75
7.1 Concept de PTS.	75
7.2 Fondement d'une PTS	77
7.3 Bénéfices.	78
7.4 Modèle pour la conception d'une PTS	79
7.5 Classification des systèmes	81
7.6 Industrialisation du modèle	83
7.6.1 <i>Typologie documentaire des PTS</i>	83
7.6.2 <i>Package complet</i>	84
7.7 Exemple de structure d'une PTS	84
7.7.1 <i>Extrait de contenu</i>	84
7.7.2 <i>Forme</i>	85
7.7.3 <i>Exemple de règles et de recommandations</i>	87
Chapitre 8 – Plateforme d'audit technique.	89
8.1 Expression du besoin	89
8.2 Conception de la plateforme	90
8.3 Outils	92

8.4	Utilisation en environnement d'entreprise	93
8.5	Exemples de scénario.	97
8.5.1	Scénario général	97
8.5.2	Scénario détaillé	97
Chapitre 9 – Mécanismes d'authentification et audit des mots de passe.		101
9.1	Inventaire applicatif	102
9.2	Mécanismes d'authentification et vulnérabilités	103
9.2.1	Messagerie	103
9.2.2	Services web	107
9.2.3	Domaine Windows	108
9.3	Audit des mots de passe	109
Chapitre 10 – Logs management.		113
10.1	Politique de gestion des logs	113
10.2	Rôles et responsabilités.	114
10.3	Périmètre de la gestion des logs	115
10.4	Format des enregistrements	115
10.5	Directive d'implémentation	116
10.5.1	Recommandations générales	116
10.5.2	Protection et rétention des logs	117
10.5.3	Outils, rapports et indicateurs	117
10.5.4	Revue des logs	118
10.6	Mise en œuvre de la gestion des logs	119
10.6.1	Critères de sélection d'un outil de gestion des logs	119
10.6.2	Inventaire du périmètre et volumétrie.	121
10.6.3	Architecture et compatibilité des flux de collecte avec la politique de sécurité.	122
10.6.4	Sévérité des événements	123
10.6.5	Habilitation des accès.	125
10.6.6	Réception des alertes	126
10.6.7	Quelques idées reçues sur la gestion des logs	127
Chapitre 11 – Veille sur les vulnérabilités et gestion des patches		129
11.1	Les principales menaces	129
11.2	Veille sur les vulnérabilités	133
11.2.1	Outillage	133
11.2.2	Organisation	136

11.3	Gestion de patchs	137
11.3.1	Organisation.	137
11.3.2	Outils	140
11.4	Métriques	140
11.4.1	Exposition au risque.	140
11.4.2	Taux de couverture	141

Troisième partie – Quelques problèmes opérationnels

Chapitre 12	– Déploiement de services autour d'une PKI	145
12.1	Problématique	145
12.2	Stockage sécurisé de certificat	146
12.3	Infrastructures nécessaires	148
12.4	Applications candidates.	150
12.5	Déploiement.	154
12.6	Impacts « collatéraux »	157
Chapitre 13	– Sécurité et mobilité.	163
13.1	La mobilité, pourquoi faire ?	163
13.2	Enjeux pour la sécurité	164
13.3	Principes et niveaux de protection	167
13.4	Décomposition de la chaîne de mobilité	170
13.5	Politique de sécurité des PDA	173
13.6	Médias portables.	176
13.7	Limitation des risques liés à la mobilité	177
Chapitre 14	– Le Wi-Fi	179
14.1	Les besoins et services associés	179
14.2	Politique de base au sein de l'entreprise	182
14.2.1	L'insécurité du Wi-Fi	182
14.2.2	Security checklist	182
14.2.3	Les mécanismes de connexion	184
14.3	Étude de cas : hotspot Internet	186
14.4	Les attaques	188

Chapitre 15 – Lutte contre les messages indésirables.	193
15.1 Définitions et repères.	193
15.1.1 La difficulté de trouver une définition.	193
15.1.2 Typologie et reconnaissance d'un spam.	194
15.1.3 Les lettres d'information	196
15.2 Phénomène et évolution du spam	196
15.2.1 Motivations des spammeurs	196
15.2.2 Statistiques	198
15.2.3 Conséquences	199
15.2.4 Pourquoi reçoit-on des messages indésirables ?	201
15.2.5 Qui est responsable de la lutte contre les messages indésirables ?	205
15.3 Les techniques de filtrages et les contre-mesures	206
15.4 Les techniques d'échappement des spammeurs	212
15.5 Recommandations	216
15.6 Parades futures	217

Quatrième partie – Les moyens de contrôle

Chapitre 16 – Les tests intrusifs.	223
16.1 Préparer.	223
16.1.1 Définir les attentes	223
16.1.2 Périmètre.	224
16.1.3 Choix d'un prestataire	225
16.1.4 Organiser, coordonner, planifier	227
16.2 Définir le cadre.	228
16.3 Déroulement opérationnel.	229
16.3.1 Reconnaissance.	229
16.3.2 Cartographie et scan de ports.	229
16.3.3 Vulnérabilités réseau	230
16.3.4 Cibler les tests	230
16.3.5 La recherche d'exploit	231
16.3.6 La partie applicative	231
16.4 Analyser les résultats.	231
16.5 Plan de correction et vérifications.	233
16.6 Cas particulier des tests Télécom	233

Chapitre 17 – Les systèmes de détection d'intrusion	235
17.1 Que fait un IDS (<i>Intrusion Detection System</i>)	235
17.1.1 Définition	235
17.1.2 Fonctions	236
17.1.3 IDS versus tests intrusifs	237
17.2 Environnement et utilisation d'un IDS.	237
17.3 Les plus-values d'un IDS	239
17.3.1 Les conseils d'un innocent...	239
17.3.2 Temps réel	242
17.3.3 Tableau de bord	243
17.4 Externalisation du management d'un IDS	244
Chapitre 18 – Tableaux de bord	247
18.1 Définition d'objectifs par le questionnaire.	248
18.2 Comment utiliser ses tableaux de bord	249
18.3 Quelques problématiques	251
18.3.1 Pertinence des indicateurs	251
18.3.2 Dépendance des indicateurs	251
18.3.3 Périodicité des indicateurs	252
18.4 Mesure de conformité - PTS	253
18.5 Messagerie	254
18.6 Antivirus.	255
18.7 Wi-fi	257
18.8 Navigation web	257
18.9 Robustesse des mots de passe	259
18.10 Incidents de sécurité..	260
Bibliographie	263
Index	265

2

Missions d'un RSSI

Objectifs

- ✓ Mettre en relief la valeur ajoutée du RSSI
- ✓ Formaliser les missions du RSSI
- ✓ Donner au RSSI la structure et les moyens de l'exercice de sa fonction

On a souvent l'habitude de dire qu'un RSSI (Responsable sécurité des systèmes d'information) est un homme-orchestre, occupant tour à tour différents rôles dans les activités qu'il est amené à réaliser. Au-delà de la description des missions nous voulons amener le lecteur à s'approprier un canevas servant de base aux missions du RSSI. Ces formalisations vous aideront à supporter la stratégie informatique tout en gardant votre libre arbitre, et à générer des revenus indirects pour votre société. Elles permettront aussi et surtout de changer l'image de la sécurité afin qu'elle soit vue comme un service et non une contrainte.

2.1 LE BLUES DU RSSI...

Comment donner une définition unique du rôle et des missions d'un RSSI ? Et d'abord pourquoi faudrait-il en donner une et une seule ? Cela dépend de la formation de la personne, de son expérience en nombre d'années et en diversité, du cheminement qu'il a réalisé au sein de sa société pour la création ou l'évolution de ce poste, de la culture et du cœur de métier de son entreprise. Bien sûr en fonction du périmètre, du système d'information, de son importance pour le métier de l'entreprise on pourra dégager des axes et des points communs.

Un RSSI doit-il être porté vers les applicatifs des services support de l'entreprise, (ressources humaines, finance, achat...) ou vers les infrastructures techniques, la protection des données des clients, les applications métiers, ou encore vers la sécurité physique ?

Très certainement un peu de tout cela, ce n'est qu'une histoire de pondération, de priorité, de criticité et de l'importance qu'accorderont le business et la direction à cette fonction. On l'aura compris, si on ajoute également l'aspect juridique et le *risk management*, le champ d'action d'un RSSI est large, très large et tend encore à s'élargir avec l'importance que ce poste prend au sein des entreprises.

On peut entendre ça et là des plaintes sur la difficulté pour un RSSI d'être présent partout et d'avoir une connaissance pointue des domaines qu'il traite. Des plaintes également sur le manque de budget et de ressources humaines. Des plaintes encore sur le peu de considération, ou le peu d'implication dans la stratégie de l'entreprise ou du système d'information.

2.2 ...ET SA VALEUR AJOUTÉE

Pour parodier un vieux film on pourrait dire « **le pouvoir est en chaque RSSI** ». N'attendons pas une quelconque reconnaissance, un rattachement hiérarchique haut placé conférant de fait une autorité gagnée par les galons, une formation, un projet prestigieux plaçant la sécurité sur le devant de la scène, mais allons les chercher. Allons préempter les ressources humaines lorsqu'un risque ou une crise existe et mettons en œuvre les contre-mesures nécessaires à la protection des personnes et des biens de l'entreprise. Engageons les équipes dans une véritable *task force* créant ainsi une solidarité défensive contre les menaces qui nous entourent. Allons demander aux différents responsables du business, des infrastructures techniques ou des applicatifs d'engager budget et ressources humaines. Demandons des analyses des risques lors de l'introduction d'une nouvelle application, d'une nouvelle technologie. Aidons les personnes chargées de satisfaire des besoins fonctionnels à comprendre les risques liés aux vulnérabilités de leur infrastructure, aidons-les à minima à les identifier pour les parer ou les accepter. Faisons voir la valeur ajoutée de la mise en œuvre d'une architecture sécurisée, en démontrant toute la maîtrise technique que l'on aura in fine sur une nouvelle application ou une nouvelle technologie.

La sécurité aide à comprendre ce que l'on manipule, comment on doit le manipuler et quel service elle apporte.

La sécurité aide les exploitants, les développeurs, les chefs de projets à sortir du modèle du *cliqueur fou*. Ce modèle est né de la simplification de l'accès au système d'exploitation au travers d'interfaces graphiques pour l'administration des OS.

À la fin des années 1990 on était ingénieur système si l'on savait cliquer et remplir des cases à cocher pour mettre en œuvre une fonction du système d'exploitation.

Personne n'était vraiment à même de comprendre les conséquences de tel ou tel choix dans l'interface graphique. Cela marchait et c'était suffisant. Des trous béants étaient ouverts, des incohérences existaient et dès qu'il s'avérait nécessaire de changer un paramètre plus rien ne fonctionnait. J'exagère bien sûr un peu. Les choses ont heureusement changé, mais il existe encore des experts de type *cliqueur fou*. Non pas que nous souhaitions jouer au réactionnaire et revenir à la ligne de commande et au bon vieil éditeur ligne, revenir à l'assembleur plutôt qu'aux langages évolués, mais il faut bien le reconnaître, comprendre ce qui se passe derrière une interface graphique et savoir vérifier par des commandes basiques le paramétrage effectué est une compétence qui se fait rare.

2.3 LA STRATÉGIE DU GAGNANT-GAGNANT

C'est précisément là que la sécurité a un rôle à jouer. Non pas pour faire de chaque technicien un *gourou* mais en manquant ses interlocuteurs pour leur faire prendre conscience qu'administrer un système ne se limite pas à cliquer mais que cela suppose de comprendre et maîtriser son fonctionnement pour réviser en permanence son analyse de risque.

Au-delà de la première réaction des techniciens, un peu vexés que vous puissiez remettre en cause leur compétence, vous aurez accru leur technicité, vous les aurez valorisés, ils se sentiront beaucoup plus confiants pour gérer leur système et tout le monde sera gagnant :

- les individus,
- l'utilisateur qui disposera d'un meilleur service,
- les clients parfois directement, parfois indirectement,
- mais surtout la sécurité de l'entreprise...

Le travail du RSSI est un travail de fourmi, sur le long terme, il apprend à être patient pour changer la culture de l'entreprise, le comportement des informaticiens, des utilisateurs, et à faire rentrer la sécurité dans les habitudes de chacun.

Être RSSI, c'est aussi avoir ce type de philosophie. Bien sûr pour partager une référence commune il faut bien revenir à des définitions un peu plus *formelles* que l'on peut trouver dans les fiches de missions et de description de poste. Cependant, avant d'aborder cela tentons de résumer ce que pourrait être un RSSI.

Un homme-orchestre, c'est sûr ! Un **manager**, encore plus sûr ! Un RSSI devrait être à géométrie variable : érecteur de règles, censeur, manager du risque, prescripteur, validateur de solution, chef de programme ou de projets, auditeur, consultant interne... en bref, un fournisseur de services.

Enfin un RSSI doit être un **communiquant**. Il faut qu'il assure le marketing de la sécurité sans paranoïa, sans tenter de terroriser ses interlocuteurs sur le potentiel des menaces mais tout simplement en les amenant à penser sécurité par eux-mêmes. Pratiquer un *gavage* en diffusant des messages effrayants liés aux menaces ambiantes peut effectivement être une stratégie très court terme et utilisée pour créer un électrochoc sur une période limitée. Ce sera à coup sûr un échec sur le moyen et le long terme car cela se retournera contre la sécurité et on aboutira indubitablement vers une perte de confiance. Agiter des épouvantails pour faire peur ne devrait donc être utilisé qu'avec parcimonie et dans des cas bien spécifiques.

De la pédagogie, de la patience, de l'enthousiasme et un réel apport de service feront oublier le mot **contrainte**.

Contrainte sécuritaire ! Quels vilains mots ! L'association du mot contrainte et du mot sécurité met à l'abri celui qui les prononce d'apporter toute explication car c'est la loi que l'on exprime ainsi. Mais, il y a la loi et l'esprit de la loi...

Si ces « contraintes » ne sont pas comprises et acceptées par les personnes devant les mettre en œuvre, par les personnes devant les subir (de leur point de vue) alors vous pouvez être sûr qu'elles seront contournées. Leur adhésion est indispensable. Adhésion ne signifie pas consensus ou compromis, c'est une démarche volontaire pour suivre une règle, une consigne, un comportement pour la protection des personnes et des biens de l'entreprise. Il y aura toujours des personnes qui ne désireront pas entrer dans le *cercle*. Des réfractaires pour lesquels le temps, les arguments et toute la conviction que vous pourrez mettre dans vos propos n'auront aucun effet.

Qu'importe, pourvu que cette population soit minoritaire. Ces individus se trouveront isolés, marginalisés, au fur et à mesure que la culture sécurité se diffusera au sein de l'entreprise.

À ce propos, et comme nous l'avons dit plus haut, le RSSI ne peut avoir le contrôle de tout et sur tout.

Alors il faut se servir de relais sécurité, pas forcément *officiels* au niveau de l'organisation, mais des relais ayant un pouvoir de persuasion et de ralliement, écoutés par leurs collègues, se chargeant de diffuser les messages sécurité pour vous. C'est connu, nul n'est prophète en son pays, c'est donc parfois des messages indirects que doivent recevoir les personnels d'une entreprise pour que l'impact soit plus fort et plus durable.

2.4 FORMALISATION DES RÔLES ET MISSIONS

2.4.1 Cadre général

Les bonnes pratiques de la sécurité définissent des **missions** qui sont au nombre de cinq :

- Définition et évolution des exigences de sécurité pour **rester en adéquation** avec les besoins business.
- Définition et mise en œuvre des solutions opérationnelles et techniques pour **garantir la politique de sécurité** des systèmes d'information.
- **Exploitation au quotidien** des solutions de sécurité et réaction sur incident.
- **Contrôle, suivi et audit** de la bonne application des mesures de sécurité.
- **Sensibilisation et formation** permanentes à la problématique sécuritaire, auprès des différents intervenants dans les systèmes d'information.

Ces missions doivent couvrir les quatre domaines de la sécurité :

- La **confidentialité** de l'information : s'assurer que les informations sont accessibles par des personnes autorisées et seulement par elles.
- La **disponibilité** et la pérennité de l'information : garantir l'accès à une information dans un temps et un délai donné.
- L'**intégrité** de l'information : s'assurer que l'information lue n'a pas subi des modifications non souhaitées.
- La **traçabilité** de l'information : pouvoir identifier les actions réalisées sur l'information.

2.4.2 Cadre individuel

Le RSSI peut être rattaché hiérarchiquement à différentes entités de l'entreprise. Le rattachement à la direction générale peut-être fait au sein de très grandes entreprises mais avec un rôle beaucoup plus large tendant plus vers le management du risque de la société toute entière.

Nous nous intéresserons ici plus particulièrement à un RSSI rattaché à la DSI (Direction des systèmes d'information). Ce RSSI assure la mise en œuvre de la politique de sécurité globale à travers un rôle d'initialisation, de coordination et de cohésion des **PTS** (Politiques techniques de sécurité) applicables au système d'information géré par la DSI.

Il est de son domaine de responsabilité de :

- Définir les exigences de sécurité applicables à l'ensemble du système d'information (SI) sur la base de la **politique de sécurité globale** de la société et des PTS.
- Contrôler et aider à la bonne application des exigences de sécurité globales et techniques sous forme d'audits formels ou ponctuels.
- Réagir aux incidents de sécurité et coordonner leur traitement dans le cadre de la procédure d'escalade lorsque leur niveau de gravité le nécessite.
- Définir les indicateurs de qualité et les tableaux de bord de sécurité dans les différents domaines techniques et fonctionnels.

- Chiffrer le coût et budgétiser la sécurité du SI, globalement et par domaine technique et fonctionnel.
- Définir annuellement les orientations sécurité de la DSI et les plans d'actions correspondants.
- Vérifier périodiquement et adapter si nécessaire les exigences de sécurité globales et techniques.
- Arbitrer, ou faire arbitrer, en cas de litige entre acteurs opérationnels et techniques, sur l'application d'une exigence de sécurité.

Afin de pouvoir exécuter l'ensemble des objectifs décrits ci-dessus et orienter son travail, le RSSI aura besoin de connaître la stratégie de l'entreprise.

Les orientations économiques et stratégiques de la société et de la DSI font partie des composants permettant de réaliser une analyse des enjeux pour déterminer les risques encourus. Des propositions de solutions de sécurité opérationnelles et techniques pour la DSI seront alors élaborées et exécutées sous le contrôle du RSSI qui a toute autorité pour leur mise en œuvre. Afin d'essayer d'être le plus exhaustif possible des audits organisationnels et techniques aideront le RSSI à détecter des vulnérabilités qui auraient échappé à l'analyse de risque. La communication relative à l'état d'avancement des travaux sécurité est primordiale pour que les acteurs opérationnels restent impliqués et ne se déchargent pas sur le RSSI.

Comme la qualité, la sécurité est l'affaire de tous. Ce lieu commun est parfois à double tranchant dans la mesure où si c'est l'affaire de tous, chacun peut penser que l'autre s'occupera des aspects sécuritaires. Nous risquons ainsi d'arriver à ce que la sécurité ne soit l'affaire de personne. C'est pourquoi cette fonction doit être là en support des entités opérationnelles de la DSI et pas seulement en acteur.

Les relais du RSSI au sein des équipes opérationnelles doivent l'alerter d'une nécessaire évolution des exigences de sécurité lorsque cela a un impact sur le service rendu, sur les besoins du business ou encore lorsque certaines règles ne sont plus en accord avec l'activité.

Les architectures, les solutions opérationnelles de sécurité à mettre en œuvre devront également répondre aux différentes obligations légales vis-à-vis desquelles la société et la DSI sont responsables.

Comme nous l'avons déjà exprimé par ailleurs la communication du RSSI est capitale, tant il se doit de faire connaître et vulgariser son travail afin de le rendre accessible à ses interlocuteurs. On pourra donc ajouter à ses fonctions :

- Définir les campagnes de sensibilisation des différents acteurs du système d'information géré par la DSI.
- Animer les différentes réunions du groupe de projet sécurité de la DSI.
- Centraliser et rediffuser les informations et incidents de sécurité survenus en interne.

- Centraliser et rediffuser les informations et alertes en provenance de sources externes.
- Centraliser et analyser les tableaux de bord sécurité des différents domaines.
- Acquérir la connaissance des besoins des utilisateurs, voire les devancer pour faire évoluer les processus sécurité du SI.

2.4.3 Le mandat du RSSI

Le cadre général et le cadre individuel ayant été fixés, il est intéressant de vulgariser la mission sécurité sous la forme d'un descriptif simplifié pouvant d'une part servir de carte de visite et d'autre part donner un formalisme, une légitimité et une autorité au RSSI qui feront de lui le garant de la politique de sécurité du système d'information.

Description de la mission sécurité

Objectifs : définir, implémenter, et contrôler la politique technique de sécurité basée sur la politique de sécurité interne.

Domaines & applications concernées : toutes les entités de la DSI ainsi que certaines unités opérationnelles de la société avec un focus particulier sur les infrastructures techniques.

Tâches :

- *L'organisation :*
 - Définition des directives de sécurité : exigences techniques, formalisation et déploiement.
 - Implémentation des politiques techniques de sécurité en s'appuyant sur des experts techniques dirigés dans le cadre de l'autorité conférée.
 - Préemption de ressources humaines des entités opérationnelles de la DSI dans la limite des objectifs individuels de chacun.
 - Approbation des choix techniques des projets stratégiques et des contrats d'externalisation en regard des exigences sécurité.
 - Centralisation et diffusion des informations relatives à la sécurité.
- *Le contrôle :*
 - Contrôle, vérification et mesure de l'efficacité et du bon rendement des solutions et de leur implémentation.
 - Simulation éventuelle d'alertes de sécurité ou d'attaques.
- *L'exploitation :*
 - Définition des procédures d'escalade et le management de cellule de crise si nécessaire.
 - Aide aux entités opérationnelles à définir le plan de sécurité informatique, la confidentialité des données et leur intégrité au niveau opérationnel et au niveau de la DSI.
 - Définition et mise en place des indicateurs sécurité et des tableaux de bord.

- *Relations internes/externes* :
 - Management de la Security Task Force.
 - Représentation de la DSI au sein des groupes de travail des autres entités de l'entreprise (juridique, ressources humaines...).

Type de rapport : Mesurer les écarts entre les objectifs de sécurité et leur mise en application grâce à des indicateurs de performance.

Composition de l'équipe : Le RSSI est mandaté par le DSI et la direction. Tous les experts et les relais sont désignés par le RSSI en coordination avec leur hiérarchie le cas échéant (rôle d'animation, management transversal, attribution directe de tâche dans les missions décrites ci-dessus).

Durée : mission permanente.

Il ne restera plus qu'à ajouter les signatures du DSI et de la direction pour que ce descriptif de mission soit tout à fait complet.

En résumé

Le RSSI doit avoir un référentiel de valeurs tournant autour de la transparence, du sang-froid, de la solidarité, de l'engagement et du professionnalisme. Ces valeurs lui permettront de pérenniser l'activité sécurité.

En faisant une bonne balance entre les besoins de l'entreprise et la protection nécessaire des personnes et des biens, il ne se contentera pas d'appliquer un état de l'art mais de cultiver le service.

Son sens de l'anticipation et de la prévention lui permettra de passer d'une culture curative à une culture préventive.

Index

- A**
- audit
 - cartographie 94, 95
 - IDS 239
 - mots de passe 96, 101, 109
 - organisationnel 31
 - outils 92
 - plateforme 89
 - technique 31
 - authentification 101
 - forte 150
- C**
- carte à puce
 - accès distant 151
 - déploiement 154
 - gestion du changement 155
 - login réseau 150
 - support de l'utilisateur 156
 - certificat 146
 - charte 39
 - cadre réglementaire 41
 - information et sensibilisation 44
 - maillon fort 53
 - principe d'imputabilité 45
 - principe d'opposabilité 45
 - principe de conformité d'utilisation 45
 - principe de traçabilité 45
 - principes juridiques 40
 - PRIVATE 46
 - responsabilisation de l'utilisateur 48
 - utilisation des données de surveillance 51
- D**
- chiffrement 154
 - cybersurveillance 39
 - détection d'intrusion 235
 - HIDS 236
 - NIDS 236
 - DSI 21, 25
- E**
- EAP-TLS 181, 184
 - espionnage 166
 - externalisation 55
- F**
- FPTI (charte) 226
- G**
- gestion de l'identité 149
 - mobilité 172
 - gestion des logs
 - IDS 238
 - outil 119
 - gestion des patches 129, 137
 - outillage 140
 - taux de couverture 141
 - GPRS 163
- H**
- HIDS 236

I

IDS 235
 connexion physique 237
 externalisation du management 244
 flux chiffrés 238
 fonctions 236
 gestion des logs 238
 intrusion temps réel 242
 outil d'audit 239
 plus-values 239
 réseau sans fil 237
 tableaux de bord 243
 tests intrusifs 237
 incident 7
 sécurité 12
 indicateurs de mesures 12
 IPSec 171

K

Kerberos 108, 160
 KPI 3, 12
 incidents de sécurité 14
 risques projets 15
 sensibilisation utilisateurs 13

L

L2TP 171
 log management 113
 périmètre 115
 logbook 8
 logiciel espion 166
 logs
 centralisation 117
 consolidation 117
 erreurs 121
 format des enregistrements 115
 infrastructure de collecte 123
 politique de gestion 113
 protection et rétention 117
 rapports 125
 réception des alertes 126
 revue 118
 sévérité des événements 124
 tentatives d'accès 122
 tentatives d'accès frauduleux 122
 volumétrie 121

M

MD4 106
 MD5 106
 mécanismes d'authentification 103
 médias portables (risques et contre-mesures)
 177
 messages indésirables 193
 mobilité 163
 chaîne de ~ 170
 challenges 165
 enjeux 164
 gestion de l'identité 172
 infrastructure technique 172
 IPSec 171
 L2TP 171
 médias portables 176
 niveaux de protection 167
 protocoles de communication 171
 recommandations sécurité 177
 sécurité 163
 SSL 172
 tableaux de bord 172
 utilisateur 171

N

NIDS 236
 NTLM 108

O

OpenDNS 219
 outsourcing 56
 cahier des charges 60
 fin de contrat 59
 projet 56
 sélection du fournisseur 58

P

pare-feu 65
 administration distante 72
 administration et maintenance 71
 changement des règles 70
 contrôles et audits 73
 fonctions 65
 politique de filtrage 68
 règles de filtrage 67
 sécurité physique 69
 stratégie de redondance 70

Patch management 129
 PDA 164
 pen-testeur 223, 225
 phishing 13
 PKI 145

- certificat 146
- infrastructure 148
- listes de révocation 157

 plan de secours 29
 plateforme d'audit technique 90
 Politique technique de sécurité Voir PTS
 processus

- de sécurité 4
- entrées 9
- points critiques 11
- sorties 10

 PTS 6, 21, 29, 75

- classification des systèmes 81
- concept 75
- conception 79
- industrialisation 83
- liste 76
- package 78, 84
- recommandations 87
- règles 85, 87
- structure 84
- tableaux de bord 249

R

RBL 207
 règle de sécurité 78
 relais ouvert 204
 roadmap 4, 25

- présentation schématique 37
- volet exploitation 31
- volet opérationnel 29
- volet stratégique 27

 RSSI 17

- budget 34
- mandat 23
- rôles et missions 20

S

scénarios d'attaques 97

- gain de privilèges 98

 scoring 249
 sécurité

mobilité 163

- PDA 173

 Sender-id 217
 Shakespeare poisoning 212
 signature et chiffrement 150
 SKIP 80, 88
 smartphone 164
 SMTP 204

- vulnérabilités 203

 spam 193

- ascii art 213
- collecte d'adresse e-mail 201
- contre-mesures 206
- définition 194
- déjouer les filtres 214
- évaluation de solutions de filtrage 210
- évolution 196
- filtrage sur extension 207
- intérêt économique 201
- liste blanche 218
- liste noire 207
- listes grises 219
- parades futures 217
- recommandations 216
- statistiques 198
- techniques de filtrages 206
- typologie 194

 spammeurs

- motivation 196
- techniques d'échappement 212

 spyware 166
 SSL 172

T

tableaux de bord 247

- antivirus 255
- conception 247
- dépendance des indicateurs 251
- diagnostics 249
- identification des menaces 250
- IDS 243
- incidents de sécurité 260
- investigations 250
- messagerie 254
- mesure de conformité 253
- navigation Web 257

- objectifs 248
- périodicité des indicateurs 252
- pertinence des indicateurs 251
- PTS 249
- robustesse des mots de passe 259
- utilisation 249
- utilité 251
- Wi-Fi 257
- tests intrusifs 31, 223
 - analyse des résultats 231
 - choix d'un prestataire 225
 - exploit 231
 - FPTI 225
 - IDS 237
 - périmètre 224
 - plan de correction 233
 - reconnaissance 229
 - scan de ports 229
 - tests Télécom 233
 - vulnérabilités 230
- TKIP 181, 185
- traitement des incidents 7

U

- usurpation d'identité
 - par le client de messagerie 107
 - par le protocole SMTP 106
- utilisateur 5

V

- vulnérabilités 129
 - veille 133

W

- WEP 181
- Wi-Fi 179
 - attaques 188
 - cybercafé 187
 - hotspot Internet 186
 - insécurité 182
 - mécanismes de connexion 184
 - politique 182
 - security checklist 182
 - services associés 179
 - tableaux de bord 257



- ▶ **MANAGEMENT DES SYSTÈMES D'INFORMATION**
- APPLICATIONS MÉTIERS**
- ÉTUDES, DÉVELOPPEMENT, INTÉGRATION**
- EXPLOITATION ET ADMINISTRATION**
- RÉSEAUX & TÉLÉCOMS**

Bernard Foray

LA FONCTION RSSI

Guide des pratiques et retours d'expérience

Cet ouvrage s'adresse aux responsables de la sécurité des systèmes d'information, qu'ils aient le titre de RSSI ou qu'ils soient chargés de cette fonction au sein d'une entreprise. Il intéressera également tous ceux qui dans leur métier ont la responsabilité de veiller à la sécurisation des applications et des données de l'entreprise.

L'un des objectifs premiers de cet ouvrage est de changer l'image de la sécurité pour qu'elle ne soit plus vue comme une contrainte mais comme un service. Si tout le monde dans l'entreprise est convaincu que l'application de petits gestes quotidiens peut éviter de grands problèmes, alors le RSSI a accompli une partie de sa mission.

Cet ouvrage est construit en quatre parties :

- La **préparation** qui définit le rôle du RSSI et ses moyens d'action (processus de sécurité, roadmap sécurité, externalisation...).
- Les **principes de base** qui présentent la définition du périmètre, la défense en profondeur des systèmes et des applications, les audits, les plans de corrections des vulnérabilités du SI.
- Les **expériences opérationnelles** qui expliquent comment faire face à quatre situations réelles auxquelles sont confrontés les RSSI : l'authentification forte, la mobilité, le Wi-Fi et enfin le spam.
- Les **moyens de contrôle** (tests intrusifs, tableaux de bord...) qui permettent de s'assurer de la robustesse des protections.

BERNARD FORAY

Après avoir travaillé une vingtaine d'années pour le compte de plusieurs grands acteurs de l'informatique (IBM, Thalès, Sun...), il est depuis 2002 RSSI chez Gemalto, le numéro 1 mondial de la carte à puce. Il est certifié CISSP depuis 2005.



6639355

ISBN 978-2-10-050218-9



www.dunod.com

