ALEXANDRE **FERNANDEZ-TORO**

Sécurité opérationnelle

Conseils pratiques pour sécuriser le SI

EYROLLES

Sécurité opérationnelle

L'auteur

Alexandre Fernandez-Toro est RSSI dans un grand groupe français. Ingénieur CNAM, il a été développeur, responsable de la production, puis consultant en sécurité des SI pendant plus de dix ans. Ces expériences lui ont donné un regard très opérationnel sur la sécurité des systèmes d'information.

Une référence pour les RSSI

Pour sécuriser les systèmes d'information, certains agissent sur la technique alors que d'autres privilégient le management. Quelle que soit l'approche, les questions liées à la sécurité opérationnelle se posent très vite : quels processus mettre en place ? À quel niveau les gérer, comment les formaliser, comment s'assurer que ces processus fonctionnent correctement dans la durée ? Cet ouvrage, très pragmatique, donne des exemples concrets sur comment sécuriser un SI. Il liste les processus opérationnels à déployer en signalant les pièges concrets à éviter. Il comporte enfin un corpus documentaire complet (exemples de politiques et de procédures) pouvant être appliqué en entreprise.

En abordant des questions telles que la sécurité des réseaux, la maîtrise du cloud, les accès distants ou la surveillance du système, ce livre donne des clés pour améliorer de façon durable la maturité de la sécurité du SI.

Au sommaire

À qui s'adresse ce livre ?

- Aux responsables sécurité (RSSI) des grands comptes et des PME, ainsi qu'à leurs équipes
- Aux personnes prenant la fonction de RSSI
- Aux personnes chargées de sécuriser le SI
- Aux chefs de projet chargés de mettre en place des processus de sécurité opérationnelle
- Aux experts de la gouvernance des SI
- À toute personne intéressée par les aspects opérationnels de la sécurité de l'information

www.editions-eyrolles.com
Groupe Eyrolles | Diffusion Geodif

Code éditeur : G13963
ISBN : 978-2-212-13963-1

39 €

DANS LA MÊME COLLECTION

F. Mattatia. – **Traitement des données personnelles.**
N°13594, 2013, 188 pages.
Y. Constantinidis, M. Volle. – **Expression des besoins pour le SI.**
N°13653, 2013, 294 pages.
D. Mouton. – **Sécurité de la dématérialisation**.
N°13418, 2012, 314 pages.
A. Fernandez-Toro. – **Management de la sécurité de l'information**.
N°12697, 2012, 480 pages.
S. Bohnké. – **Moderniser son système d'information.**
N°12764, 2010, 290 pages.
A. Lupfer. – **Gestion des risques en sécurité de l'information**.
N°12593, 2010, 230 pages.

SUR LE MÊME THÈME

C. Pernet. – **Sécurité et espionnage informatique**.
N°13965, 2014, 240 pages.
A. Jumelet, S. Quastana, P. Sauliere. – **Sécurité et mobilité Windows 8 pour les utilisateurs nomades**.
N°13642, 2013, 246 pages.
M. Untersinger. – **Anonymat sur Internet**.
N°14021, 2e édition, 2014, 264 pages.

Sécurité opérationnelle

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Je dédie ce livre à tous mes collègues.

Par leurs qualités personnelles et professionnelles, ils m'infligent au quotidien une leçon de modestie et me tirent chaque jour un peu plus vers le haut.

Table des matières

Partie II – Intégration dans la norme ISO 27001

Partie III – Annexes

Avant-propos

Plusieurs approches peuvent être adoptées pour sécuriser les systèmes d'information. Selon leur culture et leur tempérament, certains responsables de la sécurité des systèmes d'information (RSSI) privilégient le management pour descendre progressivement vers la technique. À l'inverse, d'autres préfèrent lancer des actions techniques produisant directement des résultats palpables, avant de remonter progressivement vers le management. Quelle que soit l'approche, les questions liées à la sécurité opérationnelle se posent très rapidement : quels processus mettre en place ? À quel niveau les gérer, comment les formaliser, comment s'assurer que ces processus fonctionnent correctement dans la durée ? Le but de cet ouvrage est précisément de répondre de façon pratique à ces questions.

À qui s'adresse cet ouvrage ?

Cet ouvrage s'adresse d'abord aux RSSI chargés de mettre en place des processus de sécurité opérationnelle. Il intéressera aussi les chefs de projet construisant un système de management de la sécurité de l'information (SMSI) conforme à l'ISO 27001. Par ailleurs, ce livre sera utile aux personnes souhaitant formaliser les processus opérationnels liés à la sécurité. Enfin, cet ouvrage est une aide à la prise de fonction de RSSI.

Structure de l'ouvrage

Cet ouvrage est divisé en trois parties. La première présente dans le détail les principaux processus opérationnels que l'on peut mettre en place pour sécuriser le système d'information. La seconde partie aborde les normes ISO 27001 et ISO 27002, puis explique en quoi elles peuvent contribuer concrètement à augmenter le niveau de maturité de la sécurité. La dernière partie est un recueil d'exemples pratiques, illustrant très précisément les documents pouvant être rédigés en support de la sécurité opérationnelle.

Remerciements

Je remercie mon DSI pour son soutien sans faille tout le long de mon action, pour sa vision des systèmes d'information et pour ses conseils dans la rédaction de cet ouvrage.

PARTIE I

Aspects concrets de la sécurité opérationnelle

Parmi les différentes façons d'appréhender la sécurité, il y en a deux qui ressortent plus que les autres. Certains l'abordent par le management et la conformité. Ils se basent pour cela sur des référentiels tels que COBIT ou l'ISO 27001. D'autres ont une approche radicalement opposée, se fondant sur des compétences très techniques. Ils privilégient les actions techniques, affinant les paramétrages des différents dispositifs du SI, en se basant sur des guides de sécurisation technique ou sur les recommandations détaillées de consultants techniques.

Il est indiscutable que ces deux approches, bien que radicalement différentes, contribuent fortement à sécuriser le SI. Cependant, elles laissent entre elles un vide important qui rend difficile le maintien de la sécurité dans la durée. Ce vide, c'est celui de la sécurité opérationnelle. En effet, il ne suffit pas de mettre en place un dispositif de gouvernance pour assurer la sécurité, ou de paramétrer correctement un serveur pour l'empêcher de se faire pirater. C'est un ensemble de processus qu'il faut faire vivre au quotidien pour que la sécurité atteigne réellement un niveau de maturité satisfaisant.

C'est précisément ce domaine de la sécurité opérationnelle que cette partie se propose de traiter. Pour étudier cette question, nous allons

commencer par présenter les différents niveaux de sécurité généralement constatés dans les systèmes d'information. Nous passerons ensuite en revue les principaux processus opérationnels liés à la sécurité. Nous conclurons cette partie en montrant les difficultés rencontrées dans leur mise en œuvre.

Chapitre 1

Les différents niveaux de sécurité

Pour appréhender la notion de sécurité opérationnelle, mettons-nous dans la situation d'un responsable de la sécurité des systèmes d'information (RSSI) prenant sa fonction dans une entreprise. Il découvre l'organisation dans laquelle il vient d'arriver, ses métiers, ses directions, les instances qui la composent et ses différentes implantations géographiques. Il se focalisera rapidement sur le système d'information (SI) pour s'en faire une idée et savoir comment le sécuriser. Pour cela, il procédera en deux étapes. La première permettra d'évaluer le niveau de sécurité réel du système d'information, en identifiant précisément les vulnérabilités les plus graves. La seconde étape consistera à élaborer un plan de traitement des risques, énumérant tous les projets à lancer pour sécuriser le système d'information. Ce n'est qu'après ces deux étapes préalables que le RSSI pourra se lancer dans la sécurisation réelle de son SI.

Connaître le niveau de sécurité réel

Pour connaître le niveau effectif de la sécurité du SI dont il prend la charge, le RSSI commencera par rencontrer ses acteurs les plus essentiels, à commencer par le DSI, puis le responsable de la production ainsi que le responsable réseau, sans oublier la personne encadrant les administrateurs, le responsable des études et la personne en charge du support de l'assistance aux utilisateurs. Il lui faudra plusieurs entretiens avant d'obtenir une vision pertinente de l'organisation du SI. Lors de ces séances, il ne se contentera pas d'apprendre comment est organisé le SI ; il demandera à chacun, selon sa fonction et ses compétences, quelles sont les pratiques en matière de sécurité.

Après ces échanges, il aura suffisamment d'éléments pour rédiger un « rapport d'étonnement », c'est-à-dire un document mettant clairement en

évidence les failles de sécurité dans chaque aspect du SI. En somme, ce document précise le niveau réel de sécurité du SI.

Même si chaque cas est particulier, on distingue généralement trois niveaux de sécurité différents. Le niveau le plus bas peut être nommé la « zone d'humiliation ». Un niveau de sécurité un peu plus élevé équivaudrait au « niveau de sécurité élémentaire » et, enfin, le plus élevé serait le « niveau de sécurité maîtrisée ».

Les actions que le RSSI entreprendra et l'ordre dans lequel elles seront lancées dépendront beaucoup de ce niveau de sécurité. En effet, le travail ne sera pas le même s'il a affaire à un SI situé dans la « zone d'humiliation » ou si, au contraire, des processus de sécurité sont déjà installés avec une maturité avancée. La sécurité opérationnelle aura donc un visage différent selon le niveau.

Différents niveaux de sécurité

Il est très important de savoir à quel niveau de sécurité se trouve le SI dont nous avons la charge. Les trois niveaux de sécurité qui viennent d'être évoqués ont une typologie particulière, détaillée ci-après.

La zone d'humiliation

Le niveau de sécurité le plus bas peut être appelé « zone d'humiliation ». Qu'entendons-nous par-là ? C'est un état dans lequel le SI présente de nombreuses vulnérabilités connues, simples à exploiter (voire triviales), et ce, à tous les niveaux. Ces vulnérabilités sont autant de points d'exposition permettant à un attaquant de prendre très facilement le contrôle total du SI. Des attaques dans cette situation peuvent avoir des conséquences catastrophiques pour l'entreprise : destruction irréversible d'information, pillage en profondeur du patrimoine informationnel, perturbation durable des opérations.

Illustration

Pour illustrer la zone d'humiliation, on peut faire la comparaison avec un particulier qui se ferait cambrioler alors que la porte de son appartement n'est pas blindée, que sa serrure est simple et qu'au moment des faits, elle n'était même pas verrouillée. Dans ces conditions, aucune assurance n'acceptera d'indemniser ce particulier, car il n'aura pas pris les mesures minimales nécessaires pour sécuriser son appartement.

Aussi étonnant que cela puisse paraître, cette situation est très répandue.

Les systèmes d'information situés dans la zone d'humiliation correspondent généralement au signalement suivant.

- Le contrôleur de domaine est très en retard de ses correctifs de sécurité. Il est donc vulnérable à des attaques simples. De plus, l'organisation de l'annuaire n'a pas été revue depuis plusieurs années. Il est donc fort probable qu'il regorge de comptes à privilèges dont personne n'a connaissance.
- Les accès à Internet sont multiples. Les filiales ou les agences de l'entreprise ont leur propre accès, et certains services ont même des accès ADSL.
- Les postes de travail ne sont jamais patchés et les utilisateurs sont souvent administrateurs de leur machine.
- Les serveurs les plus exposés ne sont pas à jour de leurs correctifs de sécurité.
- Les mots de passe d'administration des serveurs, des bases de données, des applications ou des équipements réseau sont triviaux.
- Des listes de mots de passe en clair, et accessibles à tous, sont oubliées dans les serveurs de fichiers.
- Le cloisonnement des réseaux est faible et, s'il y en a un, les règles du pare-feu sont illisibles et, au final, extrêmement permissives.
- Les protocoles d'authentification sont triviaux.
- Aucune revue des droits système ou applicatifs n'est jamais effectuée.
- Aucune supervision spécifique à la sécurité n'est exercée.
- Les applications sont développées sans aucune prise en compte de la sécurité.
- Etc.

Les systèmes d'information situés dans la zone d'humiliation se contentent généralement de mesures de sécurité élémentaires telles que des mots de passe pour accéder au réseau et aux applications, des antivirus dans les postes de travail et un pare-feu pour filtrer les flux entre l'intérieur et l'extérieur du SI. Les mesures de sécurité s'arrêtent souvent là.

Ainsi, un système d'information situé dans la zone d'humiliation est extrêmement exposé aux actes de malveillance. En cas d'incident de sécurité, ni le RSSI, ni le DSI ni la direction générale n'ont la moindre excuse auprès des parties prenantes, car ils n'auront pas entrepris les actions élémentaires à mettre en place pour sécuriser le SI.

Exemple

Une entreprise s'étant fait voler son fichier clientèle suite à une intrusion réseau n'aura strictement aucune excuse si, après enquête, on s'aperçoit que le serveur web directement exposé à Internet ne s'était jamais vu appliquer des correctifs de sécurité et que les comptes pour administrer les bases de données avaient des mots de passe triviaux.

Niveau de sécurité élémentaire

Le niveau de sécurité élémentaire est juste au-dessus de la zone d'humiliation. Il permet au SI de résister aux attaques les plus triviales. Ne nous trompons pas, ce n'est pas parce que ce niveau est considéré comme « élémentaire » qu'il est à peine meilleur que la zone d'humiliation. Bien au contraire. L'effort pour passer de la zone d'humiliation au niveau de sécurité élémentaire est très important.

Voici les mesures de sécurité généralement constatées dans un SI situé au niveau de sécurité élémentaire.

- Les accès à Internet ont été rationnalisés, centralisés et contrôlés.
- Les systèmes les plus exposés à Internet ont été *patchés* et sécurisés.
- Les postes de travail ont aussi été sécurisés, ou sont en passe de l'être.
- Il n'y a plus de mots de passe triviaux dans les équipements les plus sensibles.
- Il existe un début de supervision de la sécurité, mais elle est encore embryonnaire. Elle se limite pour le moment à surveiller vraiment les antivirus et à jeter un coup d'œil occasionnel aux journaux du pare-feu.
- Une première revue des comptes du domaine a permis de supprimer les comptes de personnes ayant quitté depuis longtemps l'entreprise. De plus, cela a permis de retirer du groupe « administrateur du domaine » des utilisateurs qui n'avaient aucune raison d'y être.

Ces mesures contribuent à diminuer sensiblement la surface d'exposition aux menaces. Cependant, il faut être conscient qu'à ce stade, le système d'information est encore loin d'être sûr. Une personne mal intentionnée prenant le temps de le faire n'aura pas de difficulté majeure pour trouver une brèche de sécurité et concevoir une attaque ciblée.

Exemple

Prenons l'exemple d'une entreprise ayant fait l'effort de centraliser tous ses accès à Internet sur un point unique et maîtrisé, ayant sécurisé tous ses postes de travail et ayant fait en sorte que les mots de passe permettant d'administrer les serveurs soient complexes. Cette situation peut donner au RSSI une illusion de sécurité. En effet, si les hyperviseurs permettant de piloter les machines virtuelles ont été oubliés dans le projet de complexification des mots de passe (ce qui arrive souvent), il est fort probable qu'ils aient gardé des mots de passe triviaux. Aussi, malgré tous les efforts consentis pour sécuriser le SI, une personne malveillante découvrant ce mot de passe commun pourra très simplement provoquer des dégâts importants en bloquant d'un coup tous les serveurs virtuels et les traitements qui leur sont associés.

La persistance de risques résiduels sur ces SI s'explique par les carences que l'on constate généralement dans le niveau de sécurité élémentaire.

- Les règles de filtrage entre les différents réseaux et DMZ sont trop complexes, même si un premier travail de clarification a été effectué, si bien que les réseaux sont encore perméables.
- Il n'existe toujours pas de gestion fiable des identités (revues des comptes système, applicatifs, des droits, etc.). Les utilisateurs bénéficiant d'accès privilégiés aux ressources sont encore bien trop nombreux.
- Si un effort a été consenti pour adopter de bons mots de passe pour les utilisateurs, on trouve encore trop facilement des équipements système et réseau protégés par des mots de passe triviaux, ou par défaut.
- Les applications sont vulnérables aux attaques de cross site scripting, injections SQL, etc.
- Les utilisateurs et les applications accèdent toujours aux bases de données en tant qu'administrateur.
- Si les systèmes les plus exposés sont *patchés*, les plus sensibles ne le sont toujours pas.
- La supervision de la sécurité est encore artisanale.

En somme, il reste encore d'importants efforts pour arriver à un niveau de sécurité satisfaisant. Néanmoins, si, à ce stade, les atteintes graves au système d'information sont encore possibles, elles sont un peu plus difficiles à réaliser que dans la zone d'humiliation.

Nous pouvons dire que si, à ce niveau, le RSSI a fait le minimum indispensable pour sécuriser son SI, ce dernier est encore exposé à de trop nombreuses menaces. Sa responsabilité et celle de sa hiérarchie sont moins engagées, mais cela ne le dispense pas de poursuivre les efforts de sécurisation.

Niveau de sécurité maîtrisée

Dans le niveau de sécurité maîtrisée, tout ce qu'il était raisonnable de réaliser avec les moyens et le temps disponibles a été fait. Les propriétés listées ci-après dénotent un SI ayant atteint un tel niveau.

- Les informaticiens (administrateurs système et développeurs) ont acquis les bons réflexes. L'aspect le plus flagrant (mais pas le seul) est l'usage par tous de bons mots de passe.
- Les utilisateurs sont sensibilisés aux bonnes pratiques. Ils tombent moins souvent dans les pièges habituels (pièces jointes piégées, hameçonnage, etc.) et ils collaborent avec la DSI en cas d'incident.
- Des revues régulières sur les accès aux infrastructures (pare-feu, serveurs, bases de données, contrôleurs de baies, de disques, etc.) et sur les accès aux applications donnent une assurance raisonnable que seules les personnes habilitées accèdent aux ressources.

- Les points clés du SI sont surveillés, permettant de détecter et de qualifier rapidement les événements de sécurité. Ceci se fait généralement par le moyen d'un SOC.
- Chacun sait comment agir en cas d'incident de sécurité, car un processus de gestion d'incidents est formalisé, exploité et amélioré régulièrement.
- Enfin, un véritable contrôle interne de la sécurité est appliqué afin de s'assurer que les mesures de sécurité techniques sont opérationnelles et efficaces.

Ces mesures font en sorte que le SI résiste bien aux atteintes élémentaires. Pour compromettre le SI, l'attaquant doit maintenant concevoir des attaques bien plus complexes, nécessitant une véritable expertise. Et même dans ce cas, les dispositifs de surveillance et de gestion d'incidents permettent de détecter, puis de limiter l'impact de telles attaques.

Malheureusement, certaines situations chroniques dans toutes les entreprises doivent tempérer notre enthousiasme.

- La complexité atteinte de nos jours par les SI a rendu impossible une sécurisation complète.
- Même si les identités sont très bien gérées, il est impossible d'avoir la certitude absolue qu'aucun compte indûment privilégié n'est passé à travers les mailles des revues.
- Certains systèmes ou applications historiques échappent totalement à la sécurité, car ils sont tellement anciens, et les compétences pour les maintenir sont tellement absentes, qu'il est souvent plus risqué d'y toucher que de ne rien faire.
- Il arrive que certaines directions de l'entreprise résistent encore aux bonnes pratiques ; des raisons politiques nécessitent d'attendre la retraite ou la mutation de certains responsables clés pour évoluer.

Face à cette situation, le RSSI doit procéder à un inventaire de tous ces risques résiduels et, pour chacun, proposer soit leur acceptation, soit leur contournement. L'acceptation de certains risques résiduels peut être motivée par des considérations économiques, ou parce que les impacts sont jugés acceptables, ou bien encore par des considérations conjoncturelles.

Exemple

Une vieille application métier stockant dans un fichier tous les mots de passe de tous les utilisateurs est un danger important pour l'entreprise. Pourtant, s'il est prévu de remplacer cette application dans les six mois qui viennent, la direction peut parfaitement juger acceptable le fait de ne rien entreprendre pour sécuriser l'ancienne application. En effet, le coût et le risque opérationnel de modifier l'ancienne application sont disproportionnés si l'on tient compte de sa disparition prochaine.

C'est pour cette raison qu'en général, le niveau de sécurité maîtrisée est très rarement atteint. Dans la réalité, seuls quelques îlots très sensibles du SI sont portés à ce niveau.

Quels chantiers lancer ?

Considérons que l'état des lieux réalisé par le RSSI mette en évidence que le SI est dans la zone d'humiliation. La priorité numéro un du RSSI sera de quitter cette zone aussi vite que possible. Cette volonté d'en sortir doit être quasi obsessionnelle. Pour cela, il réalisera un plan d'action.

Ce plan d'action est souvent appelé « plan de traitement des risques ». Il se traduit concrètement par un document reprenant la liste de tous les projets à lancer. Un plan de traitement des risques compile un ensemble de fiches (une par lancement de projet) présentant au moins les rubriques suivantes.

- **Nom du projet :** l'idée est d'identifier très clairement le projet en question.
- **Rappel du contexte :** il s'agit ici de rappeler la situation dans laquelle se trouve le SI dans le domaine concerné, en explicitant le problème qui se pose, pour faire comprendre pourquoi le projet est nécessaire.
- **Objectifs :** les objectifs concrets à atteindre doivent être précisés de la façon la plus claire possible, pour aider à calibrer le projet.
- **Priorité :** plusieurs niveaux de priorité peuvent être attribués, en fonction de la sensibilité et de l'urgence du projet. Chacun peut définir sa propre échelle de priorité.
- **Charge :** elle permettra de provisionner les moyens nécessaires en temps, en compétences et en argent pour mener à bien le projet.
- **Précisions supplémentaires :** d'autres points peuvent être ajoutés, comme des relations d'ordre entre les différents projets, d'éventuelles dépendances, des risques particuliers, etc.

Cette liste de rubriques n'est pas exhaustive. Nous sommes ici dans le domaine classique de la gestion de projet. Rien n'empêche de compléter ce plan par un diagramme de Gantt ou un diagramme de Pert.

Quels sont concrètement ces projets de sécurité opérationnelle que l'on retrouvera dans le plan de traitement des risques ? Une réponse générique consisterait à dire que tout projet permettant de réduire la surface d'exposition aux risques a toute sa place dans ce plan.

De façon plus concrète, voici les principaux chantiers à lancer.

- **Réseaux :** ils sont devenus tellement complexes que, très souvent, personne en interne n'en connaît la topologie exacte. Dans ces conditions, il est très difficile de garantir la sécurité. La sécurité du réseau sera donc un des tout premiers chantiers à lancer.

- **Accès distants :** avec l'informatique mobile, les solutions d'accès distant se sont multipliées, si bien qu'elles ont tendance à se disperser. La DSI peine souvent à garder la maîtrise de ces accès, ce qui présente un risque important en matière de sécurité.
- **Journalisation :** elle permet soit de détecter des actes de malveillance, soit de comprendre la nature et la profondeur des attaques. En ce sens, mettre en place une journalisation bien structurée est un préalable à la gestion des incidents.
- **Mots de passe :** un autre chantier très prioritaire est celui des mots de passe car, bien que des mécanismes permettent d'imposer de bonnes pratiques dans le domaine, l'expérience montre que les mots de passe sont encore une source de vulnérabilités majeure dans les systèmes d'information.
- **Postes de travail :** alors que de nombreuses attaques ciblent le poste de travail, la seule barrière de protection est souvent l'antivirus qui, à lui seul, peine à protéger efficacement l'utilisateur. La sécurisation du poste de travail ne se limite pourtant pas à l'antivirus.
- **Gestion des antivirus :** cet outil est souvent la première ligne de défense face aux actes de malveillance. Il est donc capital qu'il soit correctement déployé et opérationnel. Nous verrons que, contrairement aux idées reçues, ce n'est malheureusement pas toujours facile.
- **Serveurs :** si les responsables des postes de travail sont réticents à sécuriser le parc, c'est encore plus vrai pour les serveurs, que les responsables de la production hésitent à protéger, de peur de générer des régressions de service. Le RSSI doit faire preuve de détermination pour sécuriser les serveurs.
- **Sauvegardes :** tous les systèmes d'information ont des dispositifs de sauvegarde des données. Cependant, peu d'exploitants testent de façon régulière les restaurations.
- **Gestion des identités et des droits :** ce domaine couvre la création/suppression des comptes ainsi que l'attribution/modification des droits. La formalisation de ces processus laisse généralement à désirer et on constate souvent des carences graves en matière de suivi des droits applicatifs.
- **Continuité de l'activité :** mettre en place un plan de continuité d'activité ou un plan de reprise d'activité est un projet à part entière qui nécessite un investissement très fort de la DSI et des métiers. Il est très fréquent que les organismes ne s'impliquent pas autant qu'il le faudrait.
- **Tiers :** à l'ère de la sous-traitance et du cloud, plus un seul SI ne fonctionne en autarcie. Les tiers sont souvent amenés à opérer des pans entiers du SI. Aussi est-il capital de bien cadrer avec eux les règles et les pratiques en

matière de sécurité. Nous verrons qu'il sera nécessaire de mettre en place un processus de contrôle des tiers.

- **Cloud :** les contraintes liées au cloud sont très spécifiques et doivent être traitées le plus en amont possible.
- **Incidents de sécurité :** comme il est certain que, tôt ou tard, tout SI subira un jour un incident de sécurité, il est essentiel de savoir réagir rapidement et avec pertinence. C'est pourquoi ce chantier devra être lancé.
- **Juridique :** le RSSI est régulièrement amené à opérer des processus extrêmement cadrés réglementairement. Il est donc important de s'intéresser à la question juridique.
- **Infrastructures spontanées :** ces infrastructures, déployées spontanément par les utilisateurs, présentent de nombreux risques. Il faut savoir gérer ce phénomène.
- **Expirations bloquantes :** certificats, noms de domaines et licences, voici trois éléments pouvant poser de graves problèmes de production s'ils ne sont pas gérés correctement.
- **Sensibilisation :** s'il ne s'agit pas à proprement parler d'une mesure de sécurité opérationnelle, la sensibilisation permet de rendre les utilisateurs plus méfiants face aux pièges classiques qui leur sont tendus. De plus, la collaboration des utilisateurs est indispensable pour construire la sécurité. Un chantier de sensibilisation est donc nécessaire.
- **Audits :** les RSSI sont confrontés à des audits tellement fréquents que leur gestion est devenue un processus opérationnel à part entière.
- **Le tout-venant :** il s'agit ici de servir toutes les demandes en sécurité n'entrant pas dans le cadre de processus standards. Il faut savoir y répondre.

C'est par l'accomplissement de ces « petits » chantiers que le SI sortira progressivement de la zone d'humiliation. Il sera alors possible de passer aux niveaux de maturité plus élevés.

Les chapitres suivants détaillent chacun des chantiers évoqués précédemment. Dans le dernier chapitre, nous reviendrons sur cette classification à trois niveaux et nous la confronterons à la réalité des SI d'aujourd'hui.