Livre blanc

La conformité au service de la sécurité

Politiques, plans et procédures

intel Security

Ce livre blanc a été rédigé par :
Jeff Tucker
Expert-conseil en sécurité
McAfee® Foundstone®
Professional Services

Sommaire

Présentation

Ce livre blanc explique comment un programme de gouvernance de la sécurité informatique correctement structuré, fondé sur des politiques, des plans et des procédures bien conçus et mis en œuvre, renforce la sécurité de l'entreprise.

Beaucoup s'accordent à dire que la mise en conformité n'est pas synonyme d'une meilleure protection pour les entreprises. Cela est d'autant plus vrai si ces dernières mettent en œuvre chichement des normes de sécurité telles que NIST 800-53, ISO 2700 et PCI DSS (Payment Card Industry Data Security Standard), se contentant pour chaque contrôle du strict minimum nécessaire pour réussir les audits. Bien souvent, cette manière de procéder n'est pas délibérée, mais tient à l'incapacité de la direction à comprendre qu'il faut placer la barre beaucoup plus haut. Ce livre blanc étudie une approche de la sécurité axée sur la conformité, en s'intéressant à la norme PCI DSS bien connue et largement adoptée ainsi qu'aux principes qui doivent régir sa mise en œuvre. Que vous soyez soumis aux normes ISO, PCI ou NIST, les concepts demeurent les mêmes et s'appliquent à toutes les entreprises qui doivent se conformer aux exigences d'une norme de sécurité spécifique.

Commencer par des politiques, des plans et des procédures peut sembler paradoxal. De fait, la plupart des entreprises commencent par déployer l'environnement informatique pour soutenir leurs opérations, par l'implémentation d'un réseau, la mise en place des systèmes informatiques, la recherche de vulnérabilités, la mise en œuvre des contrôles d'accès et parfois, l'activation de la journalisation sur certains systèmes. Toutefois, comme toujours, la planification est importante. Prenez donc le temps de réfléchir et commencez par élaborer des politiques, concevoir des plans, mettre au point des documents de conception et développer des procédures. Ensuite, implémentez vos solutions informatiques.

Le socle

Pour réussir un programme de sécurité informatique, il faut avant tout des bases solides. Celles-ci doivent comprendre les éléments suivants :

1. **Charte** — Définissez les objectifs, les parties prenantes et les responsables du programme de sécurité.
2. **Gouvernance** — Après le succès rencontré par la gouvernance informatique et les comités d'audit indépendants, la gouvernance de la sécurité informatique a vu le jour en tant que discipline indépendante. Instaurez un comité de gouvernance de la sécurité pour aligner votre programme de sécurité sur les besoins de l'entreprise et l'intégrer dans l'ensemble de celle-ci. Il est communément admis que, dans ce nouveau contexte, il existe un conflit d'intérêt lorsque la sécurité relève du service informatique. Dès lors, la structure organisationnelle nécessite un réalignement, comme expliqué plus loin sous « Structure de l'organisation ».
3. **Politiques** — Décrivez en détail les politiques qui constitueront le cadre du programme.
4. **Plans, documents de conception et procédures** — Documentez les composantes nécessaires à la conception, à la gestion et au fonctionnement de l'environnement de données critiques.

Les sections qui suivent présentent en détail les principaux membres et attributions du comité de gouvernance de la sécurité. Elles décrivent en outre les politiques essentielles ainsi que les plans, documents de conception et procédures que doit prévoir le programme de sécurité informatique.

Gouvernance

L'entreprise doit présenter une structure qui favorise la réussite du programme de sécurité informatique. Un comité de gouvernance de la sécurité dont les responsabilités sont correctement définies contribue à cette réussite. Cette section passe en revue les points qui s'appliquent à la plupart des entreprises de nos jours.

Structure de l'organisation : responsable de la sécurité des systèmes d'informations (RSSI)
Le RSSI doit avoir pour supérieur hiérarchique le président-directeur général (PDG), le directeur financier (CFO), le responsable de la gestion des risques ou le directeur de la conformité. Il ne doit pas dépendre du service informatique. Le RSSI doit entre autres assumer les responsabilités suivantes :

1. Présider le comité de gouvernance de la sécurité
2. Superviser les opérations de sécurité informatique
3. Mettre en place, publier, gérer et diffuser la politique de sécurité
4. Vérifier que les plans de sécurité sont établis et vérifiés régulièrement
5. S'assurer que des procédures opérationnelles de sécurité écrites sont établies et gérées en continu

Comité de gouvernance de la sécurité
Les hauts dirigeants et les chefs de service de l'ensemble de l'entreprise doivent participer à la planification de la sécurité en tant que membres du comité de gouvernance de la sécurité. Le RSSI ou son suppléant doit présider le comité. Le comité sera notamment chargé de ce qui suit :

1. Supervision du programme de sécurité informatique
2. Orientation du programme pour qu'il réponde aux besoins en matière de sécurité de l'entreprise
3. Analyse et approbation des politiques soumises par le RSSI ou son suppléant
4. Examen et approbation du budget de sécurité.

Politiques

Il n'est pas rare que des politiques autorisent des interprétations tellement larges qu'elles ne satisfont pas les exigences imposées par les normes de sécurité ISO, NIST et PCI. C'est ce qui arrive lorsque la direction manque du leadership et de l'autorité nécessaires pour déterminer une orientation précise en matière de sécurité. Les entreprises ont tendance à rédiger des politiques très générales pour ensuite laisser aux départements individuels le soin de peaufiner les détails. Cette approche ne fonctionne pas dans le cas des politiques de sécurité, car chacune de leurs clauses (dispositions) peut alors donner lieu à des interprétations différentes et à des discussions.

Étant donné que les politiques de sécurité informatique visent à gérer et à réduire les risques, elles doivent impérativement fixer clairement les attentes. Prévoyez également des politiques plus spécifiques, centrées sur certains problèmes ou systèmes, pour colmater les brèches éventuelles entre les exigences générales et celles qui concernent des points précis. Décrivez dans le détail les exigences à respecter pour assurer la mise en œuvre de chaque politique conformément aux normes appropriées. Il est recommandé d'élaborer les politiques suivantes :

- **Politique de sécurité des informations de l'entreprise** — Cette politique s'applique à toute l'entreprise ; elle établit les exigences et les attentes de la direction en matière de protection des informations d'entreprise. Elle doit énoncer de façon claire les règles à respecter au minimum. Elle peut laisser une certaine latitude dans son application, mais sans jamais donner la possibilité de s'y soustraire ou de la contourner.
- **Politique de sécurité des données critiques (CDSP)** — Les organisations qui comptent un grand nombre d'utilisateurs de base (affaires, industrie, marketing, etc.) ne nécessitant pas des mesures de sécurité strictes mais qui gèrent des données réglementées et autres données critiques doivent concevoir une politique CDSP[1] qui couvre spécifiquement l'environnement visé par les exigences réglementaires.
- **Politiques régissant un thème de sécurité ou un système spécifique** — Utilisez ces politiques spécifiques pour compléter la politique CDSP, et prenez appui sur les normes lorsque vous rédigez les politiques propres à un thème.

Consignes générales pour l'élaboration des politiques
La conception d'une politique de sécurité, peu importe son objet, doit prendre en considération certains éléments fondamentaux. Cette section décrit les principaux points dont il faut tenir compte ainsi que les sections à inclure pour créer une politique efficace.

Orientation générale
Une bonne politique de sécurité doit définir l'orientation à suivre car les détails font toute la différence. Elle doit définir clairement les attentes ainsi que le niveau d'exigences minimales à respecter. Elle doit par conséquent être plus détaillée que les autres types de politiques. Ainsi, une politique stipulant simplement que « l'accès aux systèmes informatiques doit nécessiter l'authentification forte » ne suffira pas à faire appliquer cette dernière. De même, le fait de mentionner que « les données critiques seront protégées » n'indique pas explicitement que la protection de ces données est exigée. Pour promouvoir la sécurité, les dispositions d'une politique doivent être impératives. Celles qui sont énoncées précédemment sont trop tièdes, dans la mesure où elles ne fournissent pas des orientations claires ou ne précisent pas les exigences minimales à respecter. Voici quelques exemples de dispositions impératives :

- **Exemple 1** — L'accès des utilisateurs à l'ensemble des systèmes requiert l'utilisation d'un mécanisme d'authentification forte, adapté à la classification de sécurité du système concerné. Au minimum, l'authentification exigera un identifiant d'utilisateur unique et un mot de passe fort, mais dans certains cas, des méthodes d'authentification plus forte seront nécessaires en fonction du niveau de risque déterminé. Au minimum, les mots de passe doivent présenter un niveau de sécurité au moins égal au niveau le plus élevé stipulé : 1) par les impératifs réglementaires, 2) dans les recommandations du fournisseur, 3) par les meilleures pratiques en matière de sécurité, ou 4) dans les recommandations relatives à la gestion des risques des systèmes de données visés par l'accès.
- **Exemple 2** — Les propriétaires de données utiliseront un mécanisme de cryptographie fort pour protéger toutes les données présentant un niveau de classification de sécurité élevé. Au minimum, la mise en œuvre d'algorithmes, de modules et de composants cryptographiques doit être conforme à la norme FIPS. Le RSSI se chargera de définir, d'implémenter et de gérer les procédures écrites de gestion des clés cryptographiques, de procéder à l'examen de ces procédures au minimum une fois par an et d'y apporter les mises à jour éventuellement nécessaires.

Mise en place des plans et des procédures
Une politique doit exiger l'élaboration et la gestion continue de procédures opérationnelles de sécurité écrites. Elle doit identifier les plans de sécurité nécessaires aux fonctions stratégiques, comme la réponse aux incidents de sécurité informatique, la reprise sur sinistre, la continuité des activités, etc. Si les plans et procédures ne sont pas spécifiés comme obligatoires par la politique, la direction ne peut pas s'attendre à ce qu'ils soient créés.

Conformité et exceptions
La politique doit aborder la conformité et les exceptions. Par crainte de se mettre en défaut avec leurs propres politiques, certaines entreprises se gardent d'y inclure des dispositions impératives. Il est au contraire préférable que les clauses d'une politique soient sans équivoque et qu'elles précisent les modalités d'application de la politique ainsi que les exceptions à son application comme suit :

- **Délai de mise en œuvre des nouvelles exigences** — Les propriétaires d'un système non conforme à la présente politique à la date de publication[2] doivent soumettre un plan de sécurité au RSSI au plus tard [période définie par la politique] après la date de publication. Ce plan de sécurité décrira en détail tous les contrôles de sécurité en place, les contrôles compensatoires supplémentaires à utiliser et une feuille de route spécifiant les mesures à prendre pour mettre le système en conformité au plus tard [période définie] après la publication de la présente politique.
- **Exceptions** — Insérez une clause d'exception pour définir la procédure s'appliquant dans les cas où la mise en conformité d'un système ou d'un processus avec une politique ne serait pas possible dans les délais requis. Les exceptions doivent obéir aux principes suivants :
  1. Elles sont accordées au cas par cas.
  2. Elles sont accordées en fonction de critères définis.
  3. Elles sont temporaires, une date d'expiration devant être fixée dans la dérogation.
  4. Elles sont réévaluées à l'expiration de la dérogation.

- **Application** — Le non-respect d'une politique sans dérogation préalable doit avoir des conséquences. Stipulez les mesures d'application dans la politique, que ce soit explicitement ou en faisant référence à la politique de sécurité des informations de l'entreprise ou à la politique d'entreprise appropriée.

Politique de sécurité des informations d'entreprise
Une politique de sécurité efficace donne le ton en matière de sécurité, à l'adresse de toute l'entité, et informe le personnel[3] des attentes de la direction concernant la sécurité . Tous les membres du personnel doivent être conscients du degré de sensibilité des données et doivent connaître leurs responsabilités en matière de protection de ces données. Les normes de sécurité ISO, NIST et PCI exigent la mise en place de politiques, de plans et de procédures car l'expérience a démontré qu'en l'absence de ceux-ci, il subsiste une ambiguïté quant au niveau d'efforts, de contrôles et de mesures de sécurité attendus par la direction en vue de la protection des informations sensibles. Cette situation confuse peut se traduire par des brèches de sécurité considérables, raison pour laquelle il est important d'expliciter le plus possible les politiques.

Politique de sécurité des données critiques
Une politique CDSP aborde un thème de sécurité précis et permet de répondre aux exigences de sécurité élevées de l'environnement de données qu'elle vise. L'élaboration de son cadre d'application et sa conception doivent faire l'objet d'une attention toute particulière, comme expliqué dans cette section.

Cadre d'application
Le cadre d'application de la politique CDSP doit être clairement défini dans celle-ci. Cela ne signifie pas qu'elle doit répertorier l'ensemble des membres du personnel, processus et systèmes auxquels elle s'applique, mais qu'elle doit en fournir une définition claire.

Exemple de cadre d'application : La présente politique s'applique à l'environnement composé de l'environnement de données critiques (CDE) et des personnes, processus et composants système présents dans l'environnement CDE ou se connectant à celui-ci, ainsi que des systèmes et des membres du personnel directement chargés du traitement, du transfert ou du stockage des « données critiques ». Du point de vue technologique, l'environnement CDE fait référence au ou aux réseaux dans lesquels réside tout composant système qui traite, transmet ou stocke des « données critiques » (c'est-à-dire des systèmes de données critiques). Il comprend cependant aussi les personnes et processus qui gèrent des « données critiques ».

Conception
La politique CDSP doit se présenter sous la forme d'un document unique qui comporte une section pour chaque thème principal ou famille de contrôles correspondant aux exigences réglementaires que l'entreprise doit respecter. Ces sections comprendront une sous-section pour chaque exigence principale.

Exemple de conception : La politique de sécurité des données PCI contiendra six sections correspondant directement aux groupes de contrôle DSS répertoriés ci-dessous. Chacune de ces sections décrira les règles de mise en œuvre des exigences DSS correspondantes. Par exemple, la section « Création et gestion d'un réseau sécurisé » portera sur les exigences 1 et 2.

1. Création et gestion d'un réseau sécurisé
2. Protection des données des titulaires de cartes de crédit
3. Gestion d'un programme de gestion des vulnérabilités
4. Mise en œuvre de mesures de contrôle d'accès strictes
5. Surveillance et test réguliers des réseaux
6. Gestion d'une politique de sécurité des informations

Plans, documents de conception et procédures

Les entreprises ont besoin de plans, de documents de conception et de procédures pour mettre sur pied, gérer et faire fonctionner l'environnement de données critiques. Nombre d'entre elles perçoivent ces documents comme des tracasseries fastidieuses. Ils peuvent cependant avoir une valeur inestimable pour votre entreprise, que les exigences de sécurité à satisfaire résultent d'impératifs contractuels, comme dans le cas de PCI, ou de mesures législatives, comme pour les réglementations FFIEC (Federal Financial Institutions Examination Council), FISMA (Federal Information Security Management Act) ou HIPAA (Health Insurance Portability and Accountability Act). Veillez à créer ces documents, ne serait-ce que pour accélérer les évaluations et audits de sécurité.

Plans et documents de conception
Les plans servent à se préparer à un événement : déploiement de systèmes, développement de logiciels ou encore réponse à un incident de sécurité. Ne dit-on pas que « Ne pas planifier, c'est programmer l'échec » ? Lorsque c'est nécessaire, des documents de conception doivent compléter les plans, mais il peut aussi s'agir de documents distincts décrivant l'architecture de systèmes ou de l'environnement et la façon dont leurs éléments constitutifs s'assemblent. Les documents de conception permettent de comprendre les interdépendances entre les composants et les conséquences qu'aurait la défaillance d'un composant donné. Ils facilitent considérablement les tâches de modification d'un système, d'un réseau ou d'un environnement. Les plans et documents de conception doivent notamment couvrir les aspects suivants :

- Conception des systèmes
- Architecture de sécurité
- Architecture du réseau
- Plan de sécurité des systèmes
- Formation de sensibilisation à la sécurité
- Gestion et traitement des risques
- Réponse aux incidents liés à la sécurité des informations
- Reprise sur sinistre et continuité des activités

Procédures
Les procédures auxquelles nous faisons référence ici ne sont pas des instructions systématiques, mais expliquent comment faire fonctionner un composant ou exécuter un groupe de tâches afin d'atteindre un résultat précis. Dans les domaines techniques, des procédures décomposées en tâches peuvent être nécessaires pour aider les techniciens à effectuer des tâches compliquées. Toutefois, d'une manière générale, les auditeurs qui demandent à examiner les procédures ne s'attendent pas à recevoir le détail des tâches. Les procédures doivent contribuer à améliorer les opérations de sécurité et intégrer la sécurité au sein de domaines non gérés par le service de sécurité. La politique doit exiger que toutes les procédures relatives aux processus susceptibles d'affecter la sécurité des données soient soumises à l'examen et à l'approbation du RSSI. À titre d'exemple, il se peut que le service des opérations informatiques soit chargé de la gestion des comptes utilisateur. Comme ce processus a un impact considérable sur la sécurité, le RSSI sera tenu d'examiner et d'approuver les procédures se rapportant à ce processus et, en collaboration avec le service des opérations informatiques, de veiller à ce qu'il soit sécurisé.

Quelques conseils utiles

L'élaboration de politiques peut être une tâche fastidieuse et assez complexe, mais une fois cette première étape franchie, votre entreprise sera globalement en meilleure posture. Cette section propose quelques conseils qui vous aideront à éviter les pièges courants.

Généralités

1. Recrutez des spécialistes en sécurité rompus à la rédaction de documents techniques afin qu'ils puissent concevoir des politiques claires et précises, qui indiquent sans équivoque les orientations à suivre.
2. Évitez à tout prix les politiques de sécurité et procédures génériques, prêtes à l'emploi, ou basées sur des modèles. Elles ne répondront pas aux besoins de votre entreprise.

Politiques

1. Pour mettre au point vos politiques, fondez-vous sur une évaluation des risques fondamentaux de l'entreprise, sans tenir compte d'éventuels contrôles, protections et contre-mesures de sécurité en place. Les politiques elles-mêmes préciseront les contrôles, protections et contre-mesures de sécurité à mettre en œuvre.
2. Pour l'élaboration des politiques, faites appel à des professionnels de la gestion de la sécurité expérimentés.
3. Le RSSI doit se charger de la création des politiques de sécurité informatique.
4. Ne laissez jamais au service (informatique, opérations, centre d'assistance, etc.) auquel s'applique une politique de sécurité le soin de rédiger celle-ci. Ce service devra en revanche participer à la mise au point des procédures.

Procédures

1. Créez des procédures pertinentes pour les opérations.
2. Communiquez-les aux responsables et aux dirigeants de première ligne.
3. Lors du développement d'une procédure, assurez-vous le concours d'experts du domaine concerné.
4. Le RSSI doit examiner et approuver les procédures de sécurité des opérations.

Conclusion

Certaines exigences réglementaires nécessitent la mise en place de politiques et de procédures en matière de sécurité. En se conformant à ces exigences, l'entreprise renforce son programme de sécurité, à condition toutefois que les politiques soient fermes, claires et complètes. Elles doivent fixer les attentes en définissant les exigences minimales à respecter. Le fait d'intégrer des précisions sur les normes correspondantes et de les compléter par des politiques relatives à un thème de sécurité ou système précis permet de développer les exigences et d'apporter plus de clarté. Une structure organisationnelle où le RSSI ne dépend pas du service informatique élimine les conflits d'intérêt et améliore l'intégrité. Enfin, la mise en place d'un processus de gouvernance de la sécurité permet d'intégrer une sécurité efficace dans l'ensemble de l'entreprise.

L'auteur

Jeff Tucker est expert-conseil pour McAfee Foundstone Professional Services. Il est diplômé de la Bellevue University (Nebraska), où il a décroché une maîtrise en sciences de gestion de la sécurité ainsi qu'une licence en sciences, avec une spécialisation en systèmes informatiques axée sur la gestion des réseaux web. Il est responsable de la gamme de services de conformité PCI et FISMA au sein de l'équipe des services-conseils en stratégie. Jeff Tucker est notamment détenteur des certifications CISA, CISSP, QSA et MCSE. Il est directeur des missions pour les équipes d'évaluation des contrôles de sécurité, composées d'analystes de bases de données, de spécialistes des tests de la sécurité du réseau, d'experts en tests d'intrusion dans les applications web et d'évaluateurs de la conformité.

À propos de McAfee Foundstone Professional Services

McAfee Foundstone Professional Services est une division de McAfee, qui fait partie d'Intel Security. Elle propose des services et des formations assurés par des experts dans le but d'aider les entreprises à protéger, de façon continue et mesurable, leurs actifs les plus importants contre les menaces les plus critiques. Par une approche stratégique de la sécurité, McAfee Foundstone identifie et implémente, suivant un équilibre optimal, les technologies, le personnel et les processus requis pour gérer les risques numériques et optimiser les investissements en sécurité. L'équipe Professional Services se compose d'auteurs et d'experts reconnus en matière de sécurité informatique, qui bénéficient d'une vaste expérience glanée tant auprès de grandes entreprises multinationales que dans le secteur public ou les forcées armées. **http://www.mcafee.com/fr/services/mcafee-foundstone-practice.aspx**

À propos d'Intel Security

McAfee fait désormais partie d'Intel Security. Avec sa stratégie Security Connected, son approche innovante de la sécurité optimisée par le matériel et son réseau mondial de renseignements sur les menaces Global Threat Intelligence, Intel Security consacre tous ses efforts à développer des solutions et des services de sécurité proactifs et éprouvés, qui assurent la protection des systèmes, des réseaux et des équipements mobiles des entreprises et des particuliers du monde entier. Intel Security associe le savoir-faire et l'expérience de McAfee aux innovations et aux performances éprouvées d'Intel pour faire de la sécurité un élément essentiel de chaque architecture et plate-forme informatique. La mission d'Intel Security est de permettre à chacun de vivre et de travailler en toute confiance et en toute sécurité dans le monde numérique. **www.intelsecurity.com**.

1. Ces politiques pourraient être intitulées politiques de sécurité des données FISMA, GLBA, HIPAA ou PCI.
2. Date à laquelle le comité de gouvernance de la sécurité a approuvé et signé la politique en vue de sa mise en œuvre.
3. Par « personnel », on entend les employés à plein temps et à temps partiel, les intérimaires, les sous-traitants et les consultants qui « résident » sur le site de l'entité ou ont accès à son environnement de données, ses réseaux et ses systèmes.

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com