Pourquoi et Comment Adapter une Politique de Sécurité pour les Entités du CNRS

Nicole Dausque,
UREC - Unité Réseau du CNRS
Nicole.Dausque@urec.cnrs.fr

Anne Facq
CRPP - Centre de Recherche Paul Pascal
Anne.Facq@crpp-bordeaux.cnrs.fr

Gabrielle Feltin
LORIA - Laboratoire Lorrain de Recherche en Informatique et ses Applications
Gabrielle.Feltin@loria.fr

Françoise Gazelle
Observatoire de Besançon
Francoise.Gazelle@obs-besancon.fr

Olivier Servas
ATILF - Analyse et Traitement Informatique de la Langue Française
Olivier.Servas@atilf.fr

Résumé

Après une brève présentation de la genèse et des objectifs du groupe de travail CAPSEC « Comment Adapter une Politique de Sécurité pour les Entités du CNRS », nous verrons pourquoi il est important qu'une entité définisse sa PSSI « Politique de Sécurité du Système d'Information » , quelles sont les différentes méthodes étudiées par le groupe CAPSEC et quelle démarche a été utilisée par ce groupe pour générer des documents aidant les entités du CNRS à définir leur PSSI.

Ensuite nous détaillerons les étapes que doit suivre une entité pour étudier et mettre en place sa PSSI.

Enfin, nous décrirons des mises en œuvre des documents CAPSEC dans des laboratoires du CNRS puis de l' université de Franche-Comté.

Mots clefs

Sécurité, confidentialité, disponibilité, intégrité, BS 7799, ISO 17799, EBIOS, PSSI, SI, politique de sécurité informatique, besoins de sécurité, objectifs de sécurité, principes de sécurité, règles de sécurité, menaces, vulnérabilités, risques, enjeux, informations sensibles.

1 Contexte

D'une part, compte tenu de la complexité et de l'hétérogénéité du SI « *Système d'information* » (pléthore de logiciels, nombre croissant d'utilisateurs, développement du nomadisme), il s'avère nécessaire d'utiliser des méthodes pour recenser et classifier exactement ce qu'il faut sécuriser, par rapport à quoi (menaces potentielles internes et/ou externes), dans quel contexte et comment.

D'autre part, en partant du constat qu'il n'existe pas de PSSI « *Politique de Sécurité du Système d'Information* » clairement définie dans les entités du CNRS, alors que de nombreux documents issus des CERTs « *Computer Emergency Response Team* » [1] ou de l'UREC « *Unité RÉseau du CNRS* » [2], des séminaires et écoles thématiques [3] incitent au respect de la politique de sécurité en vigueur, un réel besoin de formalisme se fait sentir, d'autant plus que cette notion devient courante dans tous les organismes.

L'objectif du groupe de travail CAPSEC « *Comment Adapter une Politique de Sécurité pour les Entités du CNRS* » est la rédaction de documents permettant d'aider les entités du CNRS à définir leur propre politique de sécurité. L'entité peut être un laboratoire, un institut, une unité, une équipe de recherche du CNRS. Le terme entité pourra être généralisé à une structure d'un organisme de recherche et/ou de formation.

Le groupe CAPSEC, créé à l'initiative de Gabrielle Feltin et Françoise Gazelle, a été validé par l'UREC en Juin 2003 dans le cadre d'un groupe de travail du CNRS. Ce groupe est constitué de 5 coordinateurs sécurité[1] [4] CNRS provenant d'entités à structure différente (UMR, UMS, UPR, UPS, multi tutelle) et d'un conseiller de la DCSSI [5] « *Direction Centrale de la Sécurité des Systèmes d'Information* », Matthieu Grall.

[1] Les coordinateurs sécurité CNRS coordonnent les actions sécurité informatique et réseaux au niveau de groupes de laboratoires (généralement sur une région) et assurent la liaison entre les entités nationales CNRS (UREC et Fonctionnaire de Sécurité de Défense) et les laboratoires

2 Pourquoi une PSSI ?

Une PSSI permet à une entité d'avoir une approche méthodique et systématique pour garantir une sécurité homogène de son SI, de plus, l'étude de la PSSI est l'occasion pour une entité :

- De mesurer l'importance stratégique de son SI pour l'accomplissement de ses missions démontrant ainsi la nécessité de le sécuriser afin de protéger les résultats de recherche (articles avant leur publication, brevets, contrats industriels..) et de conserver ses savoir-faire
- De prendre conscience des menaces pesant sur son SI et de définir les mesures et moyens à mettre en oeuvre pour le protéger ou pour diminuer les impacts des intrusions
- De rédiger et d'organiser des procédures de reprises des services en cas de problèmes matériels ou d'intrusion.

Une PSSI est également un document de dialogue entre les différents acteurs du SI (instances décisionnelles, responsables d'équipes de recherche ou de services, membres de l'entité, le ou les ASR « *Administrateur Système et Réseau* » du service informatique, intervenants extérieurs, prestataires de services). Il est important que les personnels de l'entité participent au pilotage de la sécurité et donc ne la subissent pas.

À l'issue de ce dialogue, un consensus doit se dégager autour de la PSSI afin de définir une gestion des risques en fonction des moyens que l'entité peut ou doit investir dans la sécurisation de son SI et en tenant compte du principe qu'il ne faut pas entraver le travail des utilisateurs, mais éventuellement modifier leurs habitudes. Ils doivent pouvoir utiliser le SI en toute confiance tout en connaissant ses limites.

Dans ce but, il est important de sécuriser son SI de manière cohérente et de définir des périmètres de sécurité adaptés aux différents besoins de sécurité des membres de l'entité.

À titre d'exemple nous pouvons citer comme menaces pesant sur le SI :

- La perte d'un contrat industriel en raison de la divulgation d'un document confidentiel suite à une mauvaise gestion des accès aux données. La PSSI va alors préciser les mesures de sécurité à suivre pour protéger l'accès aux données confidentielles du SI
- Les menaces pesant sur la messagerie du SI : les virus, les pourriels (spams), l'atteinte à l'intégrité et la confidentialité des messages, la falsification de l'identité de l'émetteur. La PSSI va alors préciser les mesures de sécurité dans les principes à suivre pour gérer ces différents risques et définir les règles permettant de protéger la messagerie.

La PSSI est un ensemble de documents vivants qui doit être révisé régulièrement afin de prendre en compte les évolutions des besoins au sein de l'entité (modification de l'organisation de l'entité, de son personnel, du SI...) et des menaces nouvelles ou consécutives à ces évolutions de l'entité (enjeux, variation des besoins de sécurité...).

3 La démarche CAPSEC

De juin 2003 à janvier 2004, nous avons commencé par une étude des différentes méthodes existantes.

3.1 Les Critères Communs

Pour dégager des critères de sécurité, notre première action fut une étude des Critères Communs version 2.1, normalisés par l'ISO en 1999 ISO/IEC 15408 sous le nom « Critères Communs pour l'évaluation de la sécurité des technologies de l'information » [6].
Ils fournissent des critères d'évaluation de la sécurité des systèmes d'informations.
Ils traitent de la protection des informations contre leur divulgation, modification ou perte d'usage non autorisés (confidentialité, disponibilité et intégrité).
Ils définissent le contexte général de la sécurité : « La sécurité a trait à la protection des biens contre les menaces, ces dernières étant classées selon leur potentiel de nuisance envers les biens protégés ».
Ils permettent de déterminer un vocabulaire et des concepts communs à tous les acteurs de la sécurité.

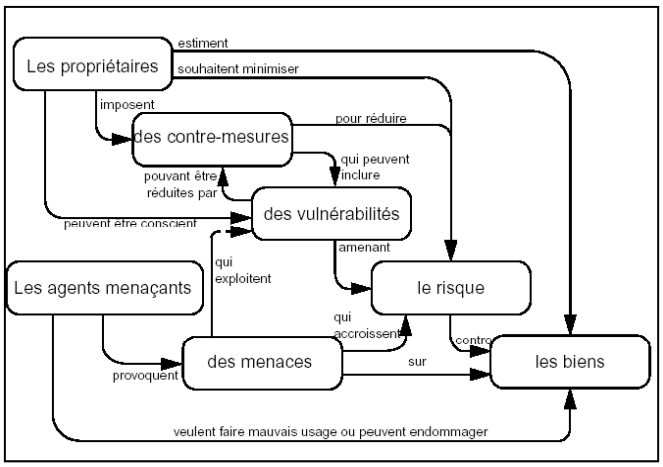

Figure 1- *Concepts de sécurité et relations*

Pour réaliser les objectifs de sécurité identifiés, la cible de sécurité doit définir clairement quelles sont les fonctionnalités de sécurité qui doivent être implémentées :

- Audit de sécurité
- Communication
- Support cryptographique
- Protection des données de l'utilisateur
- Identification et authentification
- Protection de la vie privée
- Protection des fonctions de sécurité

– Utilisation des ressources
– Chemins et canaux de confiance.

Les critères communs proposent une approche méthodique et cohérente pour examiner la façon dont est prise en compte la sécurité (cf la Figure 1). Cette approche exige en particulier que les objectifs de sécurité aient été définis au préalable pour que l'on puisse apprécier, grâce à l'évaluation, la manière dont les fonctions de sécurité parviennent à les satisfaire.

3.2 Les normes

ISO/IEC 13335 [7] : Guidelines for the Management of the IT Security. C'est un guide du management de la sécurité informatique. Il se décompose actuellement en 5 rapports techniques ISO TR 13335 :

– Définition, modèle et concepts de base
– Information sur l'organisation à prévoir dans l'entité (management et planification)
– Approche générale de la gestion de la sécurité des SI
– Guide de choix des mesures préventives
– Recommandations sur la sécurité des réseaux.

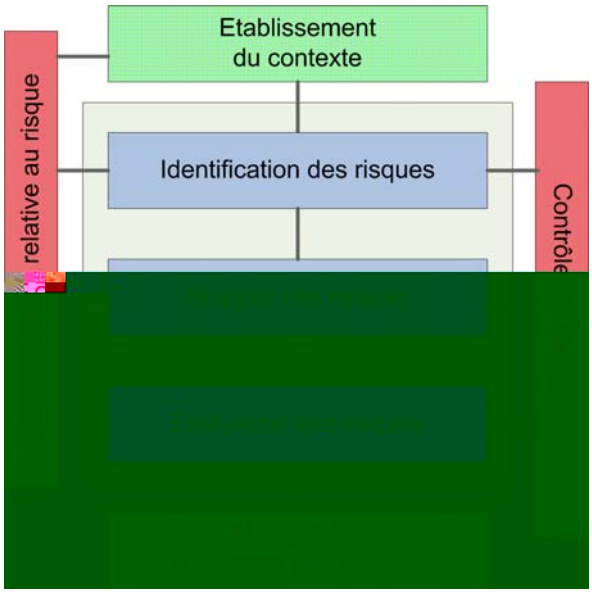

Figure 2 - *Synthèse du processus de management du risque (ISO 13335-2)*

Une partie va devenir norme internationale (IS pour International Standard) :

– ISO/IEC IS 13335-1 : Concept et management pour la sécurité
– ISO/IEC IS 13335-2 : Techniques de gestion de risques (cf la Figure 2).

Une autre partie restera sous forme de rapports techniques.

La norme d'origine anglaise BS 7799-2:2002 dont la première partie a été normalisée par l'ISO « *International Organization for Standardization* » sous la référence **ISO/IEC 17799:2005** : contient les codes de bonnes pratiques pour la sécurité de l'information et des contrôles qui y sont liés [7] .

Elle a pour objectif d'établir un label de confiance pour la sécurité globale de l'information.

Elle propose un ensemble de mesures de sécurité organisationnelles et techniques.

Elle se compose de 11 chapitres et intègre 133 mesures de contrôle.

Elle développe des points structurants de la sécurité (cf la Figure 3):

– L'appui nécessaire de la direction pour la mise en place d'une politique de sécurité et l'identification des moyens correspondants
– L'identification des menaces propres à l'entité et la pondération des risques
– La classification des informations pour ne protéger efficacement que ce qui est nécessaire
– L'organisation à mettre en œuvre.

Chaque chapitre présente une thématique de sécurité détaillée en sous-chapitres, qui sont structurés autour :

– D'activités (par exemple pour le personnel : recrutement, formation, gestion des incidents)
– D'objets (par exemple pour la sécurité physique : périmètre de sécurité, équipement)
– D'un mélange des deux (par exemple pour l'exploitation : validation de système, virus, sauvegarde, gestion des réseaux, support, échanges).

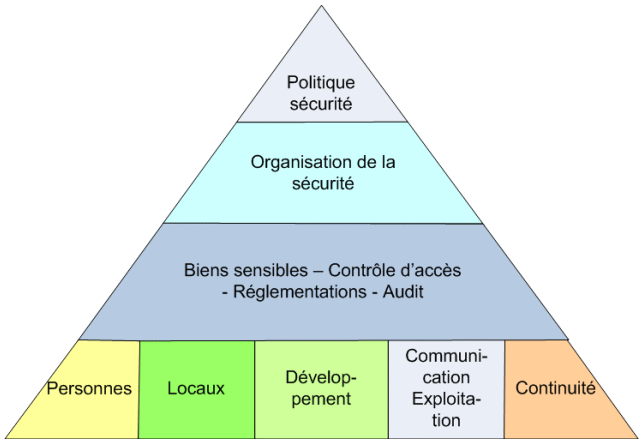

Figure 3- *Architecture de la norme ISO 17799*

Chacun de ces chapitres présente des objectifs de sécurité, des recommandations sur les mesures à mettre en œuvre et des contrôles à effectuer.

Cette norme ISO/IEC [7] requiert d'autres méthodologies pour établir la liste des biens sensibles, la liste des menaces et une analyse de risques.

3.3 Méthodes d'analyse de risques

Pour mettre en œuvre une politique de sécurité, il faut définir les objectifs de sécurité.
Or seule une méthode permet d'obtenir **une vision globale et cohérente de la sécurité** ; c'est un outil qui offre la possibilité d'**analyser**, de **concevoir**, d'**évaluer** ou de **contrôler**, ensemble ou séparément, la **sécurisation des systèmes d'information** ; il donne le moyen d'analyser et de hiérarchiser les enjeux, les objectifs de sécurité, les menaces et les vulnérabilités et de proposer des parades adaptées ; il intègre une base de connaissances.

MEHARI « *MEthode Harmonisée d'Analyse des Risques* » proposée par le CLUSIF [8] « *Club de la sécurité des systèmes d'information français* ».

La méthode a été conçue pour les grandes entreprises et les organismes afin de mettre à disposition des règles, modes de présentation et schémas de décision. L'objectif de la méthode est de proposer un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de pallier au mieux les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

Le modèle de risque MEHARI se base sur :

- Six facteurs de risque indépendants : trois influant sur la potentialité du risque et trois influant sur son impact
- Six types de mesures de sécurité (structurelles, dissuasives, préventives et de protection, palliatives et de récupération) chacune agissant sur un des facteurs de risque.

Un logiciel (non gratuit) d'assistance à la démarche est proposé par la société BUCSA.

La méthode ne possède par de déclinaison par type de métiers, d'entreprise ou d'organisme.

EBIOS « *Expression des Besoins et Identification des Objectifs de Sécurité* » [9] est une méthode de gestion des

stratégique, une partie politique (principes) et une partie technique (règles) :

- La note de stratégie de sécurité comporte : une présentation de l'entité, de son SI, des enjeux du SI, d'éléments de stratégie (référentiel réglementaire applicable, échelle de besoins, menaces retenues…)
- Les principes de sécurité s'articulent en principes organisationnels, principes de mise en œuvre et principes techniques
- Les règles de sécurité sont des règles d'application donnant entre autres les informations techniques permettant de satisfaire les principes de sécurité ; pour les écrire nous nous sommes appuyés en grande partie sur les documentations et recommandations techniques existantes de l'UREC.

En résumé, entre janvier 2004 et juin 2005 le travail du groupe CAPSEC a consisté en :

- La réalisation d'une étude EBIOS générique pour les entités du CNRS
- La rédaction d'une fiche d'enquête
- L'établissement d'un schéma de circulation des données entre les acteurs du SI
- Le recensement des enjeux pour les entités du CNRS
- L'établissement de la liste des données et fonctions à prendre en compte
- La détermination de l'échelle des besoins de sécurité sur les données et les services
- L'établissement de la liste des menaces retenues uniquement sur le SI
- La rédaction des principes de sécurité et des règles de sécurité.

4 Les étapes de définition d'une PSSI pour une entité

Suite au travail réalisé par le groupe CAPSEC [11], il s'avère que la définition de la PSSI pour une entité CNRS est composée de 4 étapes :

I. **Une enquête** sur les besoins de sécurité des utilisateurs du SI
II. **Une étude** des menaces pesant sur le SI
III. **Une définition** des principes de sécurité et leur validation par les instances politiques de l'entité
IV. **Une élaboration des règles** de sécurité permettant de respecter les principes.

Les deux premières étapes correspondent à la définition des besoins de sécurité pour les utilisateurs.

Les deux dernières étapes concernent la mise en place de la PSSI au sein de l'entité.

Au sein de l'entité, un Comité PSSI chargé d'étudier et d'adapter la PSSI de l'entité est tout d'abord constitué et validé par l'instance décisionnelle : il comprend des acteurs du SI de l'entité : direction, représentants des utilisateurs de l'entité, correspondant sécurité[2] [4] ou éventuellement des collaborateurs externes (CRI, …). Le nombre de participants à ce groupe peut être compris entre 5 et 10. Il doit être suffisant pour être représentatif des activités de l'entité mais pas trop élevé, car il serait alors difficile de travailler avec un groupe dont les membres sont trop nombreux.

4.1 Enquête sur les besoins de sécurité des utilisateurs du SI

L'objectif de cette étape est de déterminer le niveau de sécurité à appliquer aux données et aux fonctions (ou services au sens informatique du terme) couramment utilisées au sein de l'entité par l'ensemble des utilisateurs.

Chaque membre du Comité PSSI est chargé de remplir une enquête dans laquelle il spécifie les données et les fonctions du SI à sécuriser tout en ayant conscience des enjeux qu'elles représentent pour l'entité.

Les différents types d'enjeux établis par le groupe CAPSEC sont :

- Financiers (contrats pouvant être dénoncés car les expérimentations n'ont pas abouti en raison de problèmes de sécurité matériels ou logiciels)
- Politiques (image de marque, visibilité de l'organisme, crédibilité en rapport avec les plans stratégiques des organismes)
- Techniques (recherche spécifique et de pointe, protection et maîtrise des résultats liés aux découvertes, confidentialité et conservation des savoir-faire techniques).

La première partie de cette enquête permet à chaque membre du Comité PSSI d'exprimer le besoin de sécurité sur les types de données qu'il utilise.

Il commence donc par sélectionner et ajouter si besoin les données qu'il utilise dans la liste ci-dessous :

- Données d'authentification (mots de passe)
- Données liées à des contrats confidentiels (mise au point, résultat des contrats)
- Données liées à des savoir-faire (bases de connaissance)
- Données liées à des coopérations nationales ou internationales (rédaction d'articles)
- Données liées à l'enseignement (notes et sujets d'examen)
- Données expérimentales (résultats d'expériences)
- Données de gestion financières et comptables (XLAB, NABUCO)

[2] Le correspondant sécurité coordonne les actions sécurité informatique et réseaux dans son laboratoire en liaison avec les entités régionales (coordinateurs) et nationales CNRS (UREC et Fonctionnaire de Sécurité de Défense

– Données liées à des informations sur la sécurité
– Données nominatives (gestion des personnels)
– Données politiques ou stratégiques
– Données scientifiques labellisées « secret défense »
– Données liées à la vie privée de personnes.

Une fois la sélection des types de données effectuée, il est nécessaire de déterminer quels sont les acteurs agissant sur ces données et dans quel domaine elles circulent : soit uniquement en interne, soit en interne et à l'extérieur, ceci afin de construire le schéma de circulation des données entre les différents domaines, voire au sein d'une équipe ou en liaison avec des cloisonnements de réseaux virtuels (VLAN).

La Figure 5 représente le schéma type de circulation des données au sein d'une entité CNRS, construit par le groupe CAPSEC.

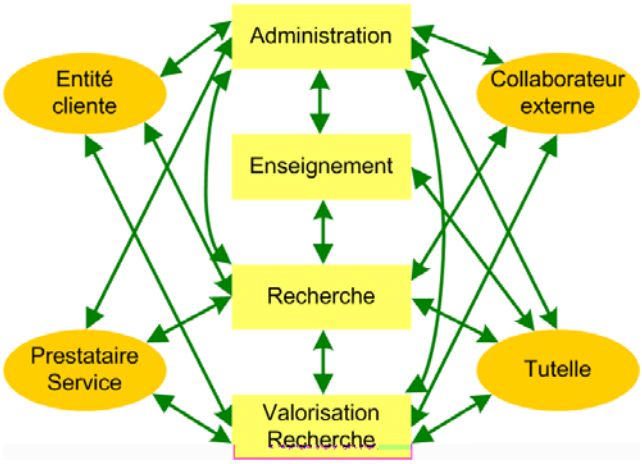

Figure 5 – *Schéma de circulation des données*

Enfin chaque membre du Comité PSSI précise le niveau de sécurité sur ces données qu'il souhaite en terme de

– Confidentialité : accessibilité de la donnée uniquement aux utilisateurs autorisés
– Disponibilité : accessibilité de la donnée au moment voulu par les utilisateurs autorisés
– Intégrité : exactitude de la donnée

en s'aidant du tableau ci-dessous, élaboré par le groupe CAPSEC.

Confidentialité	
Niveau 0 Perte de confidentialité sans conséquence	La perte de confidentialité est sans conséquence pour l'organisme (le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités à court et long terme de l'organisme). Ex : données publiques, visibles par tous
Niveau 1 Perte de confidentialité entraînant des conséquences défavorables	La perte de confidentialité entraînerait des conséquences défavorables aux intérêts de l'organisme (susceptible de provoquer une gêne dans le fonctionnement de l'organisme, cette gêne pouvant elle-même provoquer une diminution des capacités de l'organisme). Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont on protége toutes les traces écrites.
Niveau 2 Perte de confidentialité entraînant des conséquences dommageables	La perte de confidentialité entraînerait des conséquences dommageables aux intérêts de l'organisme (susceptible d'amoindrir notablement les capacités de l'organisme, avec des conséquences à plus ou moins longue échéance telles que les pertes financières, sanctions administratives ou réorganisation). Ex : données liées à un engagement de confidentialité, comme la perte de confidentialité dans un contrat dont on protége les traces écrites y compris à l'intérieur de l'entité, ou la divulgation du mot de passe
Niveau 3 Perte de confidentialité entraînant des conséquences graves	La perte de confidentialité entraînerait des conséquences graves pour l'organisme (susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières). Ex : données secret défense

Disponibilité	
Niveau 0 Délai supérieur à une semaine	Délai supérieur à une semaine, sans conséquence pour l'organisme. Ex : des services qui apportent un confort supplémentaire mais pas indispensable
Niveau 1 Délai supérieur à 8 heures et inférieur à une semaine	Ressources pour lesquelles il existe une alternative, qui entraîne une gêne ou dégradation Ex : imprimantes
Niveau 2 Délai supérieur à 2 heures et inférieur à 8 heures	Conséquences dommageables pour l'organisme, mais sans conséquence vitale humainement. Ex : arrêt du réseau, de la messagerie, données vitales non disponibles,…
Niveau 3 Délai supérieur entre temps	Ressources qui mettent en péril la vie (humaine ou animale ou biologique)

réel et 2 heures	Ex : expériences biologiques ou physiques pilotées automatiquement, système de sécurité

Intégrité	
Niveau 0 Perte d'intégrité sans conséquence	La perte d'intégrité est sans conséquence pour l'organisme (le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités à court et long terme de l'organisme). Ex : aucune vérification
Niveau 1 Perte d'intégrité entraînant des conséquences défavorables	La perte d'intégrité entraînerait des conséquences défavorables aux intérêts de l'organisme (susceptible de provoquer une gêne dans le fonctionnement de l'organisme, cette gêne pouvant elle-même provoquer une diminution des capacités de l'organisme). Ex : vérification des données, sans validation, comme des fautes d'orthographe sur une page web nuit à l'image de marque de l'entité. Ces données sont relues systématiquement.
Niveau 2 Perte d'intégrité entraînant des conséquences dommageables	La perte d'intégrité entraînerait des conséquences dommageables aux intérêts de l'organisme (susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières supérieures) Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.
Niveau 3 Perte d'intégrité entraînant des conséquences graves	La perte d'intégrité entraînerait des conséquences graves pour l'organisme (susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières supérieures). Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains).

En prenant l'exemple des données liées à des contrats confidentiels chaque membre du Comité PSSI de l'entité va répondre aux questions suivantes :

- Est-ce qu'il utilise des données liées à des contrats industriels ?
- Est-ce que ces données sont situées sur des ordinateurs situés à l'intérieur de l'entité ou sur un ordinateur à la maison ?
- Avec qui est-ce qu'il échange ces données ? Et si oui, quels sont les émetteurs et destinataires de ces données ?
- S'il perd la confidentialité sur ces données est-ce que cela a des conséquences dommageables pour l'entité ? (A priori oui, car la perte d'un contrat représente des pertes financières pour l'entité).
- Pendant combien de temps ces données peuvent ne plus être disponibles ?
- Si ces données sont modifiées (perte d'intégrité), est-ce que cela aura des conséquences dommageables ?

La deuxième partie de l'enquête permet à chaque membre du Comité PSSI d'exprimer le besoin de sécurité sur les fonctions du SI :

- Communication (ex : serveur de courrier)
- Gestion financière et comptable
- Modélisation (ex : serveur de calcul)
- Publication (ex : serveur web)
- Stockage, traitement et interprétation des données (ex : serveur de fichier).

Chaque membre du Comité PSSI indique le niveau de sécurité qu'il attend pour chacune de ces fonctionnalités, en utilisant le même tableau des besoins de sécurité que celui utilisé pour les données.

Par exemple s'il estime que le serveur de courrier ne doit pas être indisponible pendant plus de 8 heures, il va choisir le Niveau 2 comme critère de disponibilité pour ce serveur de courrier.

Une fois que chaque membre du Comité PSSI a répondu à cette enquête, une synthèse des réponses aux enquêtes doit ê(rdes ralisé0me p l(sanstim)1atrveur deedu Com)12(itetde ffusé0ms

– Défaillances techniques
– Actions illicites
– Compromission des fonctions.

Pour chaque menace, le Comité PSSI de l'entité se pose les questions suivantes :

– Est-ce que cette menace est prise en compte par exemple par la commission hygiène et sécurité (incendie, dégât des eaux…) ?
– Est-ce que l'origine de cette menace est de type environnemental, humain, naturel ?
– Est-ce que la cause de cette menace est accidentelle ou délibérée ?
– Quelle est la probabilité d'apparition de cette menace ?
– Est-ce que nous retenons ou non cette menace ?

Par exemple la menace « Écoute passive » peut être commise par un pirate, du personnel temporaire, des visiteurs qui délibérément installent par jeu ou par curiosité, des programmes permettant d'écouter ce qui se passe sur le réseau (filaire ou sans-fil) de l'entité avec des outils trouvés sur Internet qui exploitent des failles de sécurité du système d'exploitation ou des logiciels.

Cette menace peut également se produire lors des déplacements externes dans un environnement hostile, il est aussi facile pour des pirates de voler des comptes et des mots de passe.

À partir des menaces prises en compte et de la liste des vulnérabilités associées il est alors possible d'identifier les risques qui peuvent peser sur le SI, ceci en fonction de la probabilité ou de la faisabilité de réalisation d'une menace et si cette ou ces vulnérabilités identifiées sont jugées exploitables. Des scénarii d'attaques avec une probabilité associée peuvent être imaginés et donc les risques spécifiques au système.

Par exemple : un serveur web peut ne pas être configuré correctement (c'est la vulnérabilité), il est accessible de l'extérieur (c'est la faisabilité) et un programme permettant d'exploiter cette faille pour accéder et modifier les pages d'un serveur web vulnérable vient de paraître sur des sites Internet (c'est la menace) ; le risque existe donc et il est de type technique.

L'impact de la modification de la page web a pour conséquence sur l'organisme la perte d'image de marque vis-à-vis des autres organismes.

Certains risques peuvent être acceptés par les instances décisionnelles de l'entité, parce que l'entité n'a pas les moyens matériels ou humains ou parce que les moyens à mettre en œuvre sont disproportionnés par rapport à la probabilité que la menace se concrétise . Il est essentiel que chaque utilisateur en soit averti afin qu'il puisse utiliser le SI en toute confiance en connaissant parfaitement les conditions de sécurité qui y sont attachées.

4.3 Définition et sélection des principes de sécurité

Cette étape a pour but la rédaction du document fixant les orientations et les caractéristiques de la politique de sécurité de l'entité.

Pour cela, le Comité PSSI utilise la synthèse des résultats de l'enquête et de l'étude des menaces ainsi que le référentiel des principes de sécurité rédigé par le groupe CAPSEC d'après le guide de la DCSSI.

Ce référentiel comprend plus de 80 principes, regroupés en 16 domaines, classés en 3 grandes parties :

– Les Principes Organisationnels
– Les Principes de Mise en œuvre
– Les Principes Techniques.

Le Comité PSSI retient les principes pertinents pour l'entité et écarte ceux qui sont liés à des données qu'il n'a pas retenues ou des risques qu'il a choisis d'accepter.

Certains principes relèvent du schéma directeur de la tutelle de l'entité, et notamment ceux liés à l'organisation de la sécurité au niveau national, ils sont donc obligatoires.

L'action de retenir ou non un principe est fonction de la modalité d'application de chaque principe et de l'impact de cette modalité sur l'entité : coût financier des solutions matérielles et logicielles, complexité des procédures de sécurisation des données pour les membres de l'entité… Par exemple, les instances décisionnelles peuvent décider de transférer le risque à un tiers (assurance, sous-traitance, …) ou décider d'accepter le risque (par exemple dans le cas où le coût des protections est supérieur aux risques réels encourus), c'est dans ce cas une décision réfléchie et voulue au niveau stratégique, apparaissant explicitement comme telle dans la politique de sécurité.

Les principes rédigés par le groupe CAPSEC étant nombreux nous verrons ici succinctement les 15 domaines en détaillant à chaque fois un exemple de principe.

Les **Principes Organisationnels** se répartissent en 5 domaines :

– Politique de sécurité comprenant les principes tels que l'évolution, la diffusion et le contrôle de l'application de la PSSI, la protection des informations confiées à l'entité et l'adoption d'une l'échelle des besoins. Par exemple, le principe « Diffusion de la PSSI » fixe que le document décrivant la PSSI de l'entité est annexé à son règlement intérieur en veillant à réserver les informations à caractère confidentiel uniquement aux personnes concernées.
– Organisation de la sécurité contenant les principes précisant les responsabilités générales pour la sécurité du SI de l'organisme, pour l'élaboration et la mise en œuvre d'une PSSI, les modalités d'utilisation des réseaux de télécommunications externes à l'organisme,

etc…
Par exemple, le principe « Responsabilité du niveau de pilotage » précise que le pilotage de la PSSI est assuré par le directeur de l'entité.

- Gestion des risques SSI regroupant les principes permettant de définir le périmètre de gestion des risques SSI, d'identifier les objectifs de sécurité, de déterminer les circonstances qui justifient une réévaluation de la sécurité du SI, d'identifier les services justifiant l'utilisation de la cryptographie, etc…
  Par exemple, le principe « Définition du périmètre de gestion des risques SSI » indique que l'entité définit son périmètre en incluant ou non les connexions externes, les réseaux virtuels privés, le sans fil, les portables des invités ou les portables personnels.
- Sécurité et cycle de vie rassemblant les principes concernant l'intégration de la sécurité du SI dans les projets, les conditions de mise en exploitation des matériels et logiciels, la réalisation d'audits de sécurité.
  Par exemple, le principe « Réalisation d'audit de sécurité » indique que pour crédibiliser la mise en oeuvre de la sécurité informatique des audits de sécurité doivent être réalisés à l'aide d'outils spécifiques.
- Assurance et certification sont prises en compte dans le cadre de contrats où la notion de confidentialité est forte.

Les **Principes de Mise en Oeuvre** comportent 6 domaines :

- Aspects humains comprenant les principes concernant la notion d'engagement, les mesures organisationnelles pour veiller au maintien de la sécurité des éléments vitaux, la séparation des postes de travail sensibles...
  Par exemple le principe « Cloisonnement des postes de travail sensibles » adapté à une entité ayant des contrats industriels avec des contraintes de confidentialité fortes, spécifiera que les ordinateurs comportant des données confidentielles seront isolés dans un réseau séparé du réseau principal de l'entité. Lorsqu'elle adapte ce principe, l'entité peut donc aboutir à des profils d'utilisateurs plutôt qu'à un consensus global sur le principe.
- Planification de la continuité des activités précisant que l'entité doit définir un plan de continuité et des procédures permettant de maintenir les activités critiques (éventuellement dans un premier temps dans un mode dégradé).
- Gestion des incidents inclut les principes définissant les situations anormales envisageables, la maîtrise et le contrôle des incidents, la mise en œuvre des moyens de détection d'intrusions…
  Par exemple, le principe « Maîtrise des incidents » consiste à assurer la continuité de service par un matériel de secours, par une application en double.
- Sensibilisation et formation comprenant les principes concernant la documentation des responsabilités, la sensibilisation générale à la sécurité, la sensibilisation des utilisateurs aux moyens de supervision…
  Par exemple, le principe « Sensibilisation des utilisateurs au moyen de supervision » précise qu'au niveau national il existe le document « Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS » qui définit le cadre d'utilisation des fichiers de trace pour les entités du CNRS. Ce principe indique qu'il faut appliquer ce document au niveau de l'entité.
- Exploitation contenant les principes concernant la documentation des procédures d'exploitation en intégrant la SSI, l'infogérance, la maintenance et les prestations de service (sauvegardes externalisées ...), le contrôle antiviral des logiciels et données avant leur mise en exploitation, la protection et utilisation de la messagerie, etc…
  Par exemple, le principe « Règles spécifiques de filtrage aux accès » indique que le SI doit être protégé vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau.
- Aspects physiques et environnement regroupant les principes liés à la continuité de la gestion des biens physiques, à la nécessité de mettre en place une architecture sécurisée, à l'isolement des systèmes sensibles ou vitaux, à la protection de l'équipement contre le vol, etc…
  Par exemple le principe « Continuité de la gestion des bien physiques » précise qu'il est important de penser à protéger les matériels qui ne seraient pas dans les locaux sécurisés : armoire réseau ou imprimantes réseau dans les couloirs.

Les **Principes Techniques** couvrent 4 domaines

- Identification et authentification indiquant notamment que lors de l'ouverture d'un accès sur une des machines du SI pour un utilisateur, il convient d'utiliser une clé ou secret (par exemple mot de passe en faisant bien attention au choix de celui-ci) et que l'identification sur le SI pour chaque utilisateur doit être unique afin de faciliter le diagnostic en cas de problème de sécurité.
- Contrôle d'accès logique aux biens incluant les principes permettant de définir les dispositifs et procédures de protection contre les intrusions, la mise en place d'une architecture sécurisée, les attributions de privilèges d'accès aux services, etc…
  Par exemple le principe « Architecture sécurisée » indique que le recours aux moyens de chiffrement est la base en matière de sécurité des communications (SSL, SSH, IPSEC). L'usage de ces moyens est soumis au respect de la loi et de la réglementation, que les accès modems, les accès distants, les réseaux virtuels privés et les réseaux sans fil (choix du protocole 802.11i, ou accès par VPN) sont à intégrer.
- Journalisation comprenant les principes indiquant qu'il est important de mettre en place des moyens de

journalisation des intrusions et des utilisations frauduleuses, d'enregistrement des opérations et d'alerte suite à un incident de sécurité. Par exemple, le principe « Moyens de journalisation des intrusions ou des utilisations frauduleuses » précise que le SI devra comprendre des moyens, dispositifs et/ou procédures, de journalisation centralisée et protégée, de l'utilisation des services afin de détecter des intrusions ou des utilisations frauduleuses et de tenter d'identifier les causes et les origines.

- Infrastructure de gestion de clés cryptographiques comportant deux principes : « Politique de gestion des clés du CNRS » et « Protection des clés et certification »

La conclusion de cette étape est la soumission, des principes adaptés à l'entité, à la direction de l'entité et aux instances décisionnelles et consultatives (conseil scientifique, conseil de laboratoire ou conseil d'administration) qui valide ou non chacun des principes retenus ou écartés par le Comité PSSI.

4.4 Élaboration des règles de sécurité

L'objectif de cette étape est de déterminer les procédures et les solutions techniques à mettre en œuvre pour appliquer la politique de sécurité validée par la direction de l'entité.

Le (ou les) ASR de l'entité en charge de la sécurité informatique décline chaque principe de sécurité de la PSSI en procédure(s) et/ou solution(s) technique(s), il peut adapter à son entité les règles de sécurité correspondantes issues du document rédigé par le groupe CAPSEC [12].

Voici quelques exemples de règles correspondant aux principes dont nous avons parlé dans l'étape précédente :

- La règle correspondant au principe « Définition du périmètre de gestion des risques SSI » peut spécifier qu'une étude d'une architecture sécurisée d'une part, et d'autre part des différents utilisateurs du SI, doit être réalisée
- La règle issue du principe « Cloisonnement des postes de travail sensibles » pour une entité ayant des contrats industriels avec des contraintes de confidentialité fortes, pourra être : un VLAN est dédié aux utilisateurs travaillant sur ce type de contrat, de façon à protéger le stockage et l'échange de données confidentielles
- La règle liée au principe « Règles spécifiques de filtrage d'accès » peut définir que le SI de l'entité doit être protégé en filtrant les accès soit au niveau du routeur principal soit sur un garde-barrière, et que dans le cas où les accès sont filtrés par un réseau de campus, l'entité doit posséder une liste à jour des filtrages et avoir la possibilité de les faire modifier si nécessaire.

Cette étape représente l'aboutissement de l'étude sur la politique sécurité, elle permet de déterminer les solutions concrètes qui vont être mise en place au niveau de l'entité.

5 Mise en oeuvre d'une PSSI dans les laboratoires et les universités pilotes

Les documents rédigés par le groupe CAPSEC ont été testés dans les laboratoires des membres de ce groupe (ATILF, CRPP, LORIA, Observatoire de Besançon), ainsi qu'à l'IXL[3] et à l'université de Franche-Comté (après une adaptation des documents CAPSEC [12] au contexte des universités).

5.1 Mise en oeuvre dans des laboratoires du CNRS

Au CNRS, les personnes qui prennent en charge la sécurité informatique au sein des laboratoires se nomment les correspondants sécurité.

Dans chaque laboratoire pilote, le correspondant sécurité a constitué un Comité PSSI composé des représentants des acteurs du SI du laboratoire (direction, représentants des activités de recherche, représentants des services de gestion etc…) et les a réunis afin de leur présenter le document d'enquête sur les besoins de sécurité.

Les membres du comité PSSI ont parfois demandé quel était l'intérêt de l'étude d'une PSSI. Pour y répondre les correspondants sécurité ont utilisé des arguments liés au contexte de leur laboratoire. Par exemple, dans un laboratoire de chimie, le correspondant sécurité a fait un parallèle entre l'importance d'une politique en matière d'hygiène et sécurité pour la protection des personnes et l'intérêt d'une politique de sécurité informatique pour la protection de la production scientifique du laboratoire.

Les membres du Comité PSSI ou les responsables des équipes de recherche ou des services ont rempli cette enquête avec ou sans l'aide du correspondant sécurité. Une explication des termes employés dans l'enquête a été nécessaire car ces termes (intégrité, disponibilité par exemple) étaient nouveaux pour eux, des exemples de menaces sur les types de données ou de fonctions ont dû également être précisés.

Dans certains cas des ajouts de données ou de fonctions ont été nécessaires.

Après avoir recueilli les réponses aux enquêtes, le correspondant sécurité a rédigé une synthèse de ces réponses et l'a communiquée aux membres du Comité PSSI.

Ensuite, le correspondant sécurité a étudié les menaces pesant sur le SI du laboratoire avec le Comité PSSI. Il a également travaillé avec ce groupe sur la sélection des principes de sécurité adaptés au laboratoire.

---

[3] Laboratoire d'étude de l'intégration des composants et systèmes électroniques, UMR 5818, situé sur le campus de l'Université de Bordeaux I

Bibliographie

[1] CERT RENATER et CERTA
http://www.renater.fr/Securite/presentationcerts.htm
http://www.certa.ssi.gouv.fr/

[2] UREC http://www.urec.cnrs.fr

[3] vCARS http://www.urec.cnrs.fr/rubrique206.html

[4] Organisation sécurité CNRS
http://www.urec.cnrs.fr/securite/CNRS/organisation.html

[5] DCSSI http://www.ssi.gouv.fr/fr/dcssi/

[6] Critères Communs
http://www.ssi.gouv.fr/fr/confiance/methodologie.html

[7] ISO http://www.iso.org/iso/en/ISOOnline.frontpage
http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html
https://www.ihseshop.com/17799/cvm.cfm
http://www.iso.ch/
Les normes 177999 :2005 et BS 7799-2:2002 sont payantes

[8] CLUSIF
https://www.clusif.asso.fr

[9] EBIOS
http://www.ssi.gouv.fr/fr/confiance/ebios.html

[10] Guide PSSI
http://www.ssi.gouv.fr/fr/confiance/pssi.html

[11] Numéro 52 http://www.sg.cnrs.fr/FSD/securite-systemes/revue-2005.htm

[12] Doc CAPSEC
http://www.urec.cnrs.fr/securite/CNRS/recommandations_cnrs.html
https://www.urec.cnrs.fr/securite/corres-secu/CAPSEC

[13] Tableaux de bord
http://www.ssi.gouv.fr/fr/confiance/tdbssi.html

Glossaire

Attaque : action visant à remettre en cause « l'état de sécurité »

Besoin de sécurité : expression à priori des niveaux de sécurité requis de disponibilité, d'intégrité et de confidentialité associés aux données et fonctions

Confidentialité: propriétés des données et des fonctions de n'être accessibles qu'aux utilisateurs autorisés (EBIOS)

Disponibilité : propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs donnés (EBIOS)

Gestion du risque : activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque (ISO guide 7)

Intégrité : propriétés d'exactitude et de complétude des informations et des fonctions (EBIOS)

Menace : existence d'une activité potentiellement nuisible

Risque : combinaison d'une menace et des pertes qu'elle peut engendrer (EBIOS)

Vulnérabilité : faiblesse dans le système qui peut-être exploitée par une menace