Démarche PSSI générique : retour d'expérience d'établissements pilotes

Bernard Martinet
Direction du Système D'information (DiSI)
Université Joseph Fourier – BP 53 – 38041 Grenoble cedex 9

Annie Cobalto
Centre de Ressources Informatiques et du Système d'Information (CRISI)
Université de Caen Basse-Normandie
Esplanade de la paix - BP 5186 - 14032 Caen Cedex 5

Dominique Launay
RENATER, antenne de Rennes
c/o Université de Rennes 1 - CRI – 263 av. g[al] Leclerc – 35042 Rennes Cedex

Roger Negaret
Centre de Ressources Informatiques (CRI)
Université de Rennes 1
campus de Beaulieu, 263 av. g[al] Leclerc, 35042 Rennes Cedex

Résumé

Aux JRES 2009, a été présenté le principe de la fourniture d'une PSSI générique pour les établissements d'enseignement supérieur et recherche, associée à une boîte à outils permettant sa déclinaison dans chaque établissement.
Ce projet mené dans sept établissements pilotes, en utilisant une démarche implémentant la phase « planification » de la norme ISO 27001, a reposé sur les principes suivants :
- définition de périmètres communs,
- appréciation des risques en exploitant la méthode EBIOSv2,
- déclinaison des mesures sélectionnées en règles pour former la PSSI.
L'intérêt de réunir autant d'établissements était motivé par les différentes approches de la SSI qu'on peut y trouver compte tenu de leurs différences (taille, organisation administrative, sensibilisation de la gouvernance à la SSI...).
Au sein de chaque établissement différentes voies ont été recherchées pour valider la PSSI.
Cet article se propose, dans un premier temps, d'exposer une synthèse de ces travaux, qui mettent en évidence ce qui semble former les invariants d'une démarche PSSI, et les différences possibles dans les cheminements suivis ou l'appropriation des résultats obtenus.
Dans un second temps, pour trois établissements, nous décrirons plus précisément :

1. *le contexte du projet ;*
2. *le traitement des livrables ;*
3. *la mise en œuvre de la PSSI et de la gestion de la sécurité de l'information ;*
4. *les difficultés et les apports du projet.*

Mots clefs

PSSI, ISO 27001, EBIOS, SMSI

1 Le projet PSSI générique

Suite à la phase d'appel d'offres qui nous a permis de sélectionner un prestataire, les travaux en commun ont débuté le 23 janvier 2010. À cette réunion, se retrouvaient le prestataire (Fidens) et les sept établissements pilotes du projet PSSI générique (Université

de Rennes 1, Réseau Universitaire Numérique Normand (RUNN), Nancy-Université, Université de Limoges, Université de la Méditerranée, Université de Grenoble, Université de Bordeaux 1).

Le projet s'est déroulé sur quasiment un an et les derniers livrables constituant le référentiel nous ont été fournis le 17 décembre 2010. Cette livraison faisait suite aux étapes du projet qui étaient :

1. formation des équipes projet en établissement chargées d'assurer les entretiens de collecte d'information ;
2. constitution d'un référentiel commun pour assurer ces entretiens ;
3. réalisation, au sein de chaque établissement, des entretiens de contexte, de besoins de sécurité et de vulnérabilités sur trois périmètres (gestion, pédagogie et enseignement, recherche) ;
4. consolidation des données par la société Fidens ;
5. expression des scénarios de menace et identification des risques ;
6. sélection des mesures adaptées et rédaction des règles de la PSSI et des autres documents du référentiel ainsi que livraison de la PSSI propre à chaque établissement.

Le référentiel générique est constitué des documents suivants :

- une politique de management de la sécurité de l'information (PMSI) formalisant l'organisation de la gestion de la sécurité de l'information au sein de l'établissement ;
- une politique de sécurité des systèmes d'information (PSSI) détaillant les mesures issues de la norme ISO27001 retenues et leur déclinaison sous forme de règles ;
- une politique générale de la sécurité des systèmes d'information (PGSSI), document optionnel, qui, pour faciliter la validation des documents par un conseil d'administration, reprend uniquement les intitulés des mesures retenues et ne les détaille pas ;
- une matrice permettant de mettre en relation les règles de la PSSI et les mesures qu'elles déclinent ainsi que les domaines métiers impactés par ces règles ;
- une déclaration d'applicabilité type (document permettant d'indiquer quelles mesures sont sélectionnées et leur état de mise en œuvre dans l'établissement) ;
- un plan d'action type pour l'implémentation d'un Système de Management de la Sécurité de l'Information (SMSI).

Le prestataire a fourni en complément un outil, appelé « feebo », permettant d'itérer sur l'analyse de risques et éventuellement de changer de stratégie de traitement des risque, influant ainsi la sélection des mesures. Les établissements pilotes ont dû s'approprier au minimum les deux premiers documents, chacun l'adaptant à son contexte. La suite de cet article vous propose un aperçu de la variété des contextes concernant les sept établissements pilotes, puis un focus détaillé sur trois établissements en particulier : l'Université de Rennes 1, le PRES Université de Grenoble, le RUNN.

2 Synthèse des 7 projets en établissement

Dans cette partie, nous allons faire ressortir les similitudes et les différences notées durant les diverses phases du projet PSSI pour les sept établissements pilotes structurellement différents.

- 4 projets ont concerné un établissement unique, avec dans un cas un glissement vers une université unique issue d'un PRES.
- 2 projets ont concerné un PRES (un projet est resté en panne à cause de l'évolution rapide du PRES).
- 1 projet a concerné les projets mutualisés d'un ensemble inter-établissements (dans le cadre d'une Université Numérique en Région).

2.1 Organisation projet mise en place

La majorité des établissements a mis en place une organisation à deux niveaux :

- Une équipe projet formée en moyenne de 4 personnes (3 à 6) qui a réalisé les divers entretiens ; cette équipe étant parfois élargie pour la réalisation d'autres tâches telles que cartographie, validation, etc.
- Un comité de pilotage, créé spécialement pour le projet ou basé sur un comité existant.

Cette structure classique est indispensable à la bonne marche du projet.

2.2 Réalisation des entretiens d'analyse de risques

Plus ou moins étalée dans le temps, suivant la difficulté rencontrée pour établir des calendriers de rencontre, cette phase a duré de 1 à 4 mois (2,5 en moyenne). Les entretiens, quant à eux, ont été réalisés sur une durée moyenne de 1h30 (1h à 2h), ceci sans tenir compte du temps de préparation puis d'analyse et de mise en forme, ce qui porte la durée totale passée pour un entretien à une demi-journée, ou une journée complète suivant les cas. Les entretiens ont été réalisés dans la plupart des cas en tandem au niveau de l'équipe projet.

Le public interrogé et le nombre d'entretiens nécessaires varient suivant la phase de l'analyse EBIOS.

- Entretiens de contexte : en moyenne 2 entretiens réalisés auprès de Vice-Présidents (VP du Conseil Scientifique, du Conseil des Études et de la Vie Universitaire ou en charge du Système d'Information) ou de Directeurs Généraux des Services (DGS).
- Entretiens de besoins de sécurité : un nombre moyen de 23 entretiens réalisés généralement auprès de responsables de services (métiers), auxquels viennent s'ajouter des Vice-Présidents, des enseignants chercheurs ou des directeurs de laboratoire en fonction du périmètre étudié.
- Entretiens de vulnérabilités : pour une moyenne de 7, c'est le point qui voit le plus grand écart de 2 à 20, dépendant peut-être de l'organisation interne de l'établissement. Les entretiens ont été réalisés auprès des Responsables de la Sécurité du Système d'Information (RSSI), du Directeur du Système d'Information (DSI), des administrateurs systèmes et réseaux et parfois d'experts fonctionnels.

La réalisation de cette phase a nécessité une quarantaine de jours-hommes (de 12 à 65 jours-hommes en estimation suivant les établissements).

Phase essentielle de l'analyse de risques, la phase d'entretien nécessite la rencontre des acteurs au plus haut niveau de la gouvernance notamment dans la phase de contexte, où il est indispensable de rencontrer DGS et VP, à défaut du Président.

Cette phase a un plus non négligeable, c'est la prise de conscience des acteurs du niveau de sécurisation nécessaire dans leur travail quotidien.

2.3 Charge de travail totale du projet

Les estimations vont de 100 à 240 jours-hommes pour une moyenne de 160 jours-hommes.

Ce décompte de temps ne prenant généralement pas en compte le temps passé dans le groupe de travail national, il exclut toute la phase préparatoire au projet ainsi que les temps de formation. Il s'arrête après la mise en forme des documents PSSI à valider. La phase de réécriture ou de mise en forme ayant été plus ou moins importante suivant les établissements, ceci peut expliquer en partie les différences de temps passé sur le projet. Le temps nécessaire jusqu'aux validations finales par la gouvernance des établissements n'est pas pris en compte ; des validations sont encore en cours en septembre 2011.

Cette charge de travail va bien sûr être fonction de la structure de l'établissement analysé, du périmètre retenu, mais également de la finesse de l'analyse de risques produite et du détail plus ou moins important donné au document de PSSI.

2.4 Organisation de la PSSI

2.4.1 Les documents PSSI

Les documents de PMSI sont soit adaptés au contexte local, soit complètement intégrés dans le document PSSI final.

Quatre établissements ont adapté le document de PSSI générale (PGSSI) au contexte local et l'ont adopté comme document de PSSI avec dans deux cas, l'injection ou l'ajout en annexe de règles plus fines pour illustrer le document.

Le document de PSSI détaillé, est lui, soit conservé comme document de travail pour la mise en œuvre, soit instancié complètement règle après règle, soit musclé par l'addition de règles génériques déjà appliquées ou reconnues comme essentielles, avant d'être adopté comme document PSSI d'établissement.

C'est ici que l'on remarque le plus de différences entre les établissements. Elles indiquent que la notion même de ce que doit être une PSSI est appréhendé différemment selon les établissements. Cela va d'un document plus léger avec de nombreuses annexes de mise en application, à un document plus complet, pratiquement auto-suffisant.

2.4.2 Les différents comités SSI mis en place

Trois comités sont définis pour le management de la SSI : le comité de pilotage stratégique, le comité de sécurité opérationnel et le comité de liaison. Cette structure reste calquée sur celle du projet, le comité de liaison remplaçant l'équipe projet, le comité de sécurité opérationnel remplaçant le comité de pilotage. Le rôle du comité stratégique est la marque de l'engagement de la direction nécessaire au démarrage du projet de PSSI, à son maintien et son évolution.

Comité de pilotage stratégique :
Sous le contrôle du chef d'établissement ou de son représentant, il valide et gère la PSSI.
Dans trois établissements un comité spécifique a été créé. Dans les quatre autres ce rôle échoit à un comité existant. Ce comité se réunit une fois par an pour les revues de direction (ISO 27001).

Comité de sécurité opérationnel :
Il est chargé de l'évolution de la PSSI, de l'analyse des risques, des propositions de traitements des risques et de processus de suivi. Il se réunit trois à quatre fois par an.
On note deux créations pures, et une création par concaténation de comités existants. Dans les autres cas ce rôle échoit à une structure en place.

Comité de liaison :
Relais des décisions de sécurité vers les composantes, il pilote les projets de sécurité, gère les incidents, recueille les problèmes, etc. Il gère la sécurité au quotidien.
Tous les établissements se sont basés sur des structures déjà en place pour remplir ce rôle.

2.5 Outil d'analyse de risques

L'outil feebo permet de réaliser intégralement une analyse de risques ou de reprendre une analyse de risques existante, afin d'agir sur toutes les étapes de l'analyse, de l'appréciation des besoins de sécurité à la stratégie de traitement des risques. Il permet ensuite d'extraire les mesures de la norme ISO 27002 qui s'appliquent à la stratégie adoptée. De cette sélection découlent les règles de la PSSI que l'établissement appliquera.

Cet outil n'a été que partiellement testé sur l'université de Rennes 1. Une autre université (Toulon) a accepté de le tester. Il en ressort que l'outil n'est pas utilisable en l'état et mériterait une profonde refonte pour être exploitable et généralisable aux autres établissements. Il n'est donc pas fourni dans l'outillage PSSI générique et n'est utilisé à l'heure actuelle par aucun établissement.

Cet outil n'étant pas utilisable, il reste néanmoins la possibilité d'utiliser les outils qui ont servi dans le cadre de ce projet. Il s'agit de tableurs, disponibles sur la page du projet (intranet des RSSI), qui, même s'ils n'offrent pas la puissance attendue de l'outil feebo, facilitent les entretiens de besoin de sécurité et d'expression des vulnérabilités.

3 Focus sur trois établissements

Nous allons maintenant comparer la démarche dans trois établissements pilotes :

- une université : l'Université de Rennes 1
- un Pôle de Recherche et d'Enseignement Supérieur : le PRES Université de Grenoble, associant quatre universités, une école d'ingénieurs et un institut d'études politiques
- une Université Numérique en Région : l'UNR RUNN (Réseau Universitaire Numérique Normand) regroupant trois universités et deux écoles d'ingénieurs.

3.1 Contexte du projet

La décision de participer au projet PSSI générique a été prise à un niveau politique dans les trois établissements. Un facteur de motivation de la direction, à Rennes en particulier, a été le passage aux compétences élargies et la nécessité de définir un Schéma Directeur du Système d'Information (SDSI) intégrant un volet SSI.

Pour Grenoble et le RUNN le regroupement d'établissements dans une structure régionale nécessitait une gestion cohérente de la SSI dans les établissements partenaires. Pour cela, et dès leur création, ces structures avaient mis en place une organisation pour la SSI. Deux coordinateurs SSI et un Correspondant Informatique et Libertés (CIL) inter-universitaires avaient été nommés à Grenoble. Un groupe de travail comprenant les RSSI des cinq établissements et leurs adjoints avaient été créé pour le RUNN et une personne avait été recrutée pour assister ce groupe de travail.

Voici l'organisation mise en place pour le projet PSSI générique :

Équipe projet		
	Composition	Effectif
Rennes	le RSSI, le RSSI adjoint (membre de l'équipe systèmes du CRI), un responsable de cellule de proximité d'un des campus de l'université, un correspondant sécurité d'un laboratoire CNRS. Pour des raisons d'hébergement géographique, l'animateur du groupe du projet national s'est joint à cette équipe projet.	5
Grenoble	4 RSSI (ou adjoints) issus de quatre des six établissements du PRES.	4
RUNN	3 RSSI (ou adjoints) et l'assistant du groupe de travail SSI du RUNN	4

Comité de pilotage projet			
	Basé sur un comité existant	Composition	Effectif
Rennes	Oui sur celui du SDSI	Président, plusieurs Vice-Présidents (VP), Directeur Général des Services (DGS), Directeur du CRI, RSSI	9
Grenoble	Oui	Les DGS et les VP SI des 6 établissements, les 2 coordinateurs SSI inter-universitaire et le CIL	15
RUNN	Non	Deux VP et le chef de projet RUNN, représentant le comité de pilotage du RUNN, les DGS des 5 établissements, un DSI, un ingénieur hygiène et sécurité et des invités (un CIL, un représentant de la délégation régionale du CNRS) et l'équipe projet	16

L'objectif du projet était d'élaborer une PSSI par établissement pilote et une PSSI générique basée sur les sept analyses de risques et couvrant toutes les activités d'un établissement d'enseignement supérieur et de recherche. Ces activités ayant été regroupées en trois grands domaines : la pédagogie (ou enseignement), la recherche et le support à l'enseignement et à la recherche.

Pour Grenoble, prévu à l'origine pour être centré sur les parties mutualisées des établissements du PRES, le périmètre s'est rapidement étendu pour devenir le projet de PSSI générique commun à l'ensemble des établissements du PRES.

Pour le RUNN le périmètre retenu pour la PSSI a été celui des projets communs (services numériques mutualisés à destination des étudiants et des personnels, carte multiservice, points d'accès ...). Mais un deuxième objectif était d'aider les cinq établissements à élaborer leur propre PSSI à partir d'un modèle commun.

Dans le premier cas l'analyse de risques a été menée sur les parties mutualisées et sur un échantillonnage dans les établissements pour les divers métiers (ressources humaines dans un établissement, finances dans un second, etc.). Vu l'étendu du périmètre, certaines fonctions n'ont pas été détaillées, et le principe de retenir les résultats génériques obtenus par les autres établissements du groupe national a été validé.

Dans le second cas cette analyse de risques a été faite d'une part sur les projets communs en interviewant les différents porteurs de projet et d'autre part dans un seul des établissements en interviewant un échantillon de responsables métiers des trois grands domaines (pédagogie, recherche et support à l'enseignement et à la recherche). L'analyse de risques effectuée dans un seul des établissements permettait de participer plus complètement à l'élaboration de la PSSI générique.

Enfin dans un cas, où il existait déjà un comité régional de coordination SSI Universités-CNRS, la partie liée au périmètre recherche s'est cantonnée à l'administration de la recherche, les autres fonctions, notamment les PSSI de laboratoire étant déléguées à cette structure. Dans l'autre cas où cette structure n'existait pas encore, le CNRS a été associé au projet (participation du Correspondant Régional de la SSI (CRSSI) au groupe de travail régional et invitation au comité de pilotage, interview du CRSSI et d'un directeur de laboratoire mixte), l'objectif étant la mise en place d'une organisation mutualisée associant les différentes tutelles des unités de recherche et permettant une gestion efficace et cohérence de la SSI.

Voici un comparatif des entretiens réalisés pour l'analyse de risques :

	Fonction des personnes interviewés	Nombre d'entretiens	Durée totale
Rennes	VPs, responsables de service (scolarité, ressources humaines, documentation,recherche...) et directeurs de laboratoire, administrateurs systèmes, informaticiens	25	1,5 mois
Grenoble	DGS, VP SI, Agent Comptable, Directeur Financier, Directeur Adjoint Ressources Humaines, Responsable pôle RH, Chef de cabinet (communication), VP CEVU, VP étudiant, Responsable scolarité, Responsable formation & vie étudiante, Responsable Service Recherche, Directeur de Laboratoire, Directeur du Service Informatique Mutualisé, Architecte SI, Responsable pôle applications, Responsable pôle usage, RSSI	24	2 mois
RUNN	2 VP (membres du comité de pilotage), DGS (pour le pilotage et la DRH), 2 directeurs d'UFR, 1 directeur d'IUT, 1 directeur d'école d'ingénieurs, 2 directeurs de laboratoire, le Coordinateur Régional SSI du CNRS, Ingénieur Hygiène Sécurité, Responsables de services (Direction des Études et de la Vie Étudiante, Direction de la Recherche, Agence comptable, Affaires financières, Service Commun Documentation, Centre de Ressources Informatiques et du Système d'Information, Cellule TICE/FOAD, Direction Communication, Affaires Juridiques, Immobilier, médecin SUMPPS), administrateurs systèmes et réseaux + les 11 porteurs de projet du RUNN	28 + 11	2 mois

Tous ces entretiens ont été réalisés en binômes (pour Grenoble : un RSSI de l'établissement et un extérieur).

3.2 Traitement des livrables

3.2.1 La PMSI

Dans le cas des trois établissements ce document a été instancié pour adapter la description des comités aux structures en place. Il importe surtout pour la formalisation du management de la SSI mis en place.

3.2.2 La PGSSI

Pour Rennes, le document PGSSI a été adapté au contexte et complété par toutes les mesures manquantes et figurant dans la PGSSI générique, indépendamment de l'analyse de risques. L'analyse étant trop macroscopique, Rennes n'arrivait plus à faire la liaison entre analyse de risques et mesures. L'adoption d'une liste de bonnes pratiques a donc été préférée, quitte à ensuite effectuer des analyses de risques sur des périmètres très précis, permettant d'y vérifier la pertinence des mesures génériques et d'y rajouter éventuellement des mesures précises et adaptées au contexte et aux risques identifiés. Ce document représente le premier volet de la PSSI (document stratégique appelé « PSSI : principes généraux »).

Pour Grenoble, parce que la PSSI générée doit être applicable à l'ensemble des établissements du PRES, il a été décidé de ne pas entrer dans des détails qui auraient peut-être été impossible à harmoniser entre tous. Le document PGSSI a donc été retenu comme PSSI. Nous restons donc ici à un niveau d'intention décliné suivant les règles ISO 27002, pour la politique, les règles précises mises en œuvres étant décrites dans des documents annexes.

Ce document n'a pas été retenu par le RUNN.

3.2.3 La PSSI

Pour Rennes, toutes les règles ont été révisées par un comité d'experts de six à dix personnes selon les domaines abordés par les mesures. L'objectif de cette révision était d'obtenir des règles « applicables » dans toutes les situations particulières de l'université. De plus certaines règles ont fait l'objet d'une introduction pour définir le contexte et les termes employés (exemple : postes de travail gérés par le CRI, postes « université » gérés par le personnel, postes personnels connectés au réseau, etc). Ce document de 72 pages représente le second volet de la PSSI (document appelé « PSSI : règles »). Un troisième document, « PSSI : documents d'application », devra contenir tous les documents d'application auxquels il est fait référence dans les règles.

Pour Grenoble, le document de PSSI détaillé est un document de travail dans la mise en œuvre des mesures. Il sert de base pour la rédaction des documents à annexer à la PSSI.

Pour le RUNN, c'est le document de PSSI générique, document recensant tous les risques indépendamment de l'analyse de risques qui a été adapté au contexte local pour définir la PSSI du RUNN, une analyse complète n'ayant pas pu être effectuée sur tous les projets. Un résumé remplace certaines mesures de la PSSI générique en faisant référence à des documents d'application plus techniques qui restent en grande partie à écrire. Le résultat est un document de PSSI de 44 pages.

3.2.4 Validation

La validation devant être faite par le comité stratégique du SI, Rennes est en attente, en septembre 2011, de la création effective de ce comité dans le cadre de la mise en place de la Direction du Système d'Information (DSI). Il est prévu de faire valider deux documents : la PMSI, et la PSSI (elle-même sous forme de deux documents : principes généraux et règles). Le document « PSSI - règles » sera présenté au comité de pilotage stratégique par lots de règles au moment de leur mise en œuvre, ces lots étant préparés et soumis à validation par le comité de sécurité opérationnel.

La validation se fait en deux étapes à Grenoble. Le comité de sécurité opérationnel placé au niveau inter-universitaire pour assurer une évolution commune de la PSSI, valide les annexes techniques de mise en œuvre de la PSSI. Les comités de pilotage stratégiques restant du domaine de chaque établissement, valident chacun les documents PMSI et PGSSI et valideront les évolutions futures lors des revues de directions (ISO 27001). Ces documents, validés en inter-universitaire, ont été validés par 4 établissements sur 6 à ce jour.

PMSI et PSSI du RUNN ont été validés par le comité de pilotage du projet PSSI puis approuvés par le comité de pilotage de l'ensemble du RUNN comprenant notamment les présidents d'université et directeurs d'école ou leurs représentants (vice-présidents). Cette approbation finale a eu lieu environ six mois après la fourniture des livrables par le prestataire.

3.3 Mise en œuvre

3.3.1 Composition des différents comités SSI

Voici la composition des comités SSI prévus dans la PMSI (hors invités) :

Comité de pilotage stratégique			
	Basé sur un comité existant	Composition	Effectif
Rennes	Oui	Comité stratégique du SI (en création) : Président, DGS, VP finance, 2 VP, DSI	6
Grenoble	Variable suivant les établissements	Le pilotage stratégique de la SSI reste du domaine de chaque établissement. Pour le périmètre recherche il existe un comité de coordination SSI Universités-CNRS Délégation Alpes.	Variable suivant les établissements 15
RUNN	Non	Chaque établissement est représenté par son président ou directeur + une personne désignée (FSD, DGS ou DSI) + le RSSI + le chef de projet RUNN + un représentant de la délégation régionale du CNRS	17

Comité de sécurité opérationnel			
	Basé sur un comité existant	Composition	Effectif
Rennes	Non	RSSI, RSSI adjoints, Correspondant Informatique et Libertés, un représentant du service juridique, représentants de la DSI, experts invités	5 à 10
Grenoble	Oui, concaténation de comités existants	DGS, VP SI, DSI et RSSI de chaque établissement + Directeur du PRES + Directeur service informatique mutualisé	24
RUNN	Oui, le groupe de travail SSI RUNN	Les RSSI et adjoints des cinq établissements, le CRSSI du CNRS, l'assistant du groupe de travail. Chaque établissement mettra ensuite en place sa propre organisation au niveau opérationnel.	12

Comité de liaison			
	Basé sur un comité existant	Composition	Effectif
Rennes	Non	Pourrait être composé des chargés de la SSI dans les composantes et unités de recherche	~31
Grenoble	Oui	6 RSSI ou adjoints des établissements	6
RUNN	-	Pas de comité de liaison au niveau du RUNN. Chaque établissement choisira ou non de mettre en place un comité de liaison. Pour l'Université de Caen le comité de liaison est composé des chargés de la SSI dans les composantes et unités de recherche.	36 chargés de la SSI nommés à ce jour à l'Université de Caen

3.3.2 Plans d'action

À Rennes la mise en œuvre devant être discutée au sein du comité de sécurité opérationnel, celle-ci est suspendue à la mise en place officielle de ce comité. Cependant certaines règles sont déjà appliquées et d'autres devront l'être suivant un plan réparti dans le temps et des priorités étudiées par le comité de sécurité opérationnel. Des analyses de risques devront être régulièrement opérées sur des périmètres précis et restreints et les règles manquantes pour réduire les risques ainsi découverts seront alors à

mettre en œuvre. En attendant le RSSI et son adjoint démarrent une première étude de mise en œuvre sur le thème de la gestion de l'authentification qui concerne tous les usagers : définition précise des règles, mise en chantier des nouvelles versions de deux produits importants : gestion des pages Sésame, gestion des comptes extérieurs aux bases institutionnelles.

À Grenoble le comité de liaison se réunit avec une fréquence d'une demi-journée par semaine pour faire avancer la mise en œuvre. Suivant les sujets abordés des experts métiers sont ou seront consultés.

Treize chantiers PSSI, regroupés autours d'axes fédérateurs ou de métiers, ont été définis pour apporter une réponses aux 41 mesures ISO 27002 retenues par l'étude afin de refuser les risques de niveau 4 (sur une échelle de 0 à 4) mis en évidence, et ce sur un délai de 18 mois. Quatre chantiers, reposant essentiellement sur les composantes informatiques (ASR, DSI, RSSI...), sont actuellement en cours. Ils comprennent une étude des mesures de la PSSI détaillée, suivi d'une adaptation de ces mesures au contexte local si nécessaire ou d'un rejet circonstancié, et enfin une écriture des propositions de procédures à mettre en place dans les établissements en vue d'une validation en comité de sécurité opérationnel.

Les neuf autres chantiers nécessitant le concours d'experts métiers, sont pour l'instant en attente de la validation définitive des PSSI par les comités de pilotage stratégiques d'établissement et du démarrage des plans de communication communs sur la mise en œuvre de la PSSI, prévus en novembre.

Pour le RUNN la mise en œuvre et le suivi de la PMSI et de la PSSI s'appuie sur un plan d'action établi par le groupe de travail pour une première période de 15 mois (jusqu'à fin 2012). Ce plan comprend :

- l'initialisation de la nouvelle organisation conformément à la PMSI (comité de pilotage stratégique associant le CNRS et mise en place de réunions mensuelles pour le comité de sécurité opérationnel constitué des RSSI et adjoints des cinq établissements plus le CRSSI du CNRS) ;
- l'inventaire complet des biens du RUNN ;
- un travail sur la sensibilisation des acteurs dans les établissements et notamment la production de modules d'auto-sensibilisation à la SSI et leur mise en ligne sur les différentes plate-formes de formation à distance ;
- la déclinaison de la PMSI et de la PSSI dans chaque établissement en repassant par une phase d'entretiens ;
- la rédaction des documents d'application prévus dans le PSSI et la formalisation ou l'adaptation des procédures existantes aux exigences de la norme ISO 27001 ;
- la mise en œuvre de la gestion de la sécurité : tableau de bord, indicateurs, organisation des réunions ;
- la mise en œuvre du suivi et de l'amélioration continue : audits, révision des documents PMSI et PSSI, définition d'un nouveau plan d'action.

3.4 Difficultés et apports

Pour Rennes, l'étendue du périmètre traité a été une difficulté. Cela a nécessité la consolidation des besoins de sécurité en les regroupant par thème, s'éloignant ainsi du détail des besoins exprimés par les personnes interrogées.

De plus, le regroupement des périmètres « Pédagogie » et « Gestion » (dû au fait que la plupart des éléments essentiels de ces domaines sont supportés par une entité principale, la salle machines du centre de ressources informatiques) a accentué cet éloignement, rendant difficile le lien entre les besoins exprimés et les mesures retenues.

Le choix a été fait d'une tentative d'exhaustivité des mesures (telles que définies dans la 27002) avec si possible des règles de bonnes pratiques associées afin de ne rien oublier. On atteint ici les limites de l'exercice : une appréciation du risque exhaustive à l'échelle d'un établissement universitaire est difficile à appréhender.

L'apport le plus important a été de réaliser un document listant de manière exhaustive tous les sujets de sécurité auxquels l'université doit réfléchir. Les gouvernants et tous les personnels ont ainsi devant les yeux les vraies questions à se poser pour une amélioration constante de la sécurité du système d'information. La mise en place d'un comité de sécurité opérationnel et d'une instance de décision spécifique au système d'information devrait permettre d'avancer officiellement et méthodiquement sur tous ces chantiers.

Pour Grenoble, l'ensemble des difficultés provient surtout de la structure multi-établissements, qui ralentit certaines phases, comme la validation, bien qu'assurant que tout le monde avance dans le même sens.

Cet aspect inter-universitaire est également un plus, car il a permis de mutualiser les forces au niveau des RSSI, très concernés, et couvre un plus grand champ d'experts métiers consultables sur un domaine plus précis.

L'apport le plus important du projet est bien sûr la mise en place d'une gestion de la SSI, avec une réelle prise en compte des besoins, et une réelle volonté affichée par la gouvernance d'avancer sur ce domaine.

Dans le cas du RUNN, la première difficulté a été la définition du contexte et du périmètre de la PSSI dans un cadre de projet multi-établissements.

Dans la phase d'identification des biens (biens essentiels et biens supports) il a été complexe de trouver le bon niveau pour une cartographie de nos SI, compte tenu de l'ampleur du périmètre. A l'Université de Caen l'analyse de risques a porté principalement sur les biens gérés par le service informatique et sur les biens recensés lors des interviews.

Est également apparue une difficulté d'appropriation de la démarche SSI par les directions de chacun des établissements, la SSI étant souvent assimilée à la sécurité informatique et donc réduite à une affaire d'informaticiens. De leur côté, les administrateurs systèmes et réseaux (ASR) se sentent parfois dépossédés (à tort) par le RSSI de leurs missions relatives à la sécurité, ce sentiment étant entretenu par l'absence de positionnement clair du RSSI (souvent ASR lui-même) et le manque de visibilité de ses missions (absence de lettre de mission). Les ASR ont aussi parfois un sentiment d'ingérence du RSSI dans leur travail quotidien et s'inquiètent du surcroît de travail. Il a donc fallu sensibiliser, convaincre, être patient et tenace pour mener ce projet de PSSI.

Enfin ce projet a entraîné une charge de travail importante sur la durée et il a été difficile par moments de mobiliser les membres du groupe de travail en dehors des réunions, notamment pour la phase de relecture et d'adaptation des documents génériques. Cependant, ce projet a apporté une dynamique et une émulation inter-établissements et a permis de mettre en commun des moyens humains pour avancer dans l'objectif d'amélioration de la SSI des établissements. Il a provoqué une prise de conscience des risques et des responsabilités de chacun dans le domaine de la SSI, notamment au travers des entretiens et des différentes formes de communication autour du projet. Il a également permis une meilleure compréhension et reconnaissance du travail des RSSI ainsi que l'acquisition de compétences dans la gestion de la sécurité de l'information. Enfin l'organisation mise en place pour le projet va servir de base à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI).

4 Conclusion

Ce projet a le mérite de montrer qu'imaginer une PSSI pour une Université, voire même un PRES, n'est pas une lubie d'informaticien, nous l'avons fait ! L'expérience acquise, nous conforte sur la nécessité de sensibiliser la direction à la mise en place d'une gestion de la sécurité par les risques.

Bien sûr, il n'est pas question de minimiser l'étendue de la tâche, mais avec une organisation adaptée (un comité de pilotage et un groupe projet) et le soutien de la gouvernance sous forme d'attribution des ressources adéquates, votre projet aboutira. Toute la documentation accumulée lors de ce projet vous permettra même d'améliorer le processus, puisque le plus souvent, vous n'aurez qu'a vous assurer que vous suivez les schémas déjà décrits.

L'importance du contexte de l'établissement est, comme on a pu le voir au cours de cet article, primordiale. Il ne faut pas hésiter à y passer du temps. Les entretiens sont des moments privilégiés avec les utilisateurs, ils permettent de les mettre en confiance et sont de bonnes occasions de sensibilisation.

Le pragmatisme est de mise lors de tels projets et il sera probablement nécessaire d'adapter les règles de la PSSI, ainsi que l'organisation proposée dans la PMSI au contexte de votre établissement. Il n'y a rien de pire que des règles inapplicables et une organisation de projet qui ne correspond pas à la culture de votre établissement.

Enfin, après avoir hiérarchisé les mesures, formalisez leur échelonnement dans le temps au travers d'un plan d'action qui vous permettra d'évaluer leur mise en œuvre et leur efficacité.