Kit de déploiement d'une PSSI d'unité à destination des unités de recherche

Marie David, Alain Rivet, Bernard Martinet, Frédéric Sauveur, David Gras, Nicolas Garnier, Dominique Fournier, Cyril Bras

Kit de déploiement d'une PSSI d'unité à destination des unités de recherche

Marie David
CNRS Délégation Alpes - SSI
25 avenue des Martyrs
38000 Grenoble

Bernard Martinet
Université Grenoble Alpes - DGDSI
41 rue des mathématiques
38400 Saint-Martin d'Hères

Frédéric Sauveur
Institut polytechnique de Grenoble - DSI
46 avenue Félix Viallet
38000 Grenoble

Cyril Bras
CEntre de Recherches sur les MAcromolécules Végétales - CERMAV
601 rue de la chimie
38400 Saint-Martin d'Hères

Dominique Fournier
CNRS – SSI/CRIC
25 avenue des Martyrs
38000 Grenoble

Nicolas Garnier
Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés - TIMA
46 avenue Félix Viallet
38000 Grenoble

David Gras
CNRS Délégation Alpes - SSI
25 avenue des Martyrs
38000 Grenoble

Alain Rivet
CEntre de Recherches sur les MAcromolécules Végétales - CERMAV
601 rue de la chimie
38400 Saint-Martin d'Hères

Résumé

Le site grenoblois a adopté, depuis 2009, une organisation collégiale entre le CNRS et les établissements d'enseignement supérieur, pour le pilotage de la sécurité de l'information des Unités Mixtes de Recherche (80 UMR). Une réflexion sur la mise en œuvre d'une Politique de Sécurité des Systèmes d'Information (PSSI) d'unité a été initiée dès 2011, avec comme objectifs de fournir une méthode, des outils et des éléments « génériques » aux chargés de sécurité des SI de ces unités , afin de les accompagner au mieux dans leur démarche.

Trois laboratoires représentatifs des thématiques et des organisations de recherche présentes sur le site (CERMAV, LEPMI et TIMA) ont participé au projet, qui leur a permis, d'une part, de mettre en place leur PSSI et d'autre part, de fournir, à chaque étape de la démarche, les éléments communs pouvant servir de modèle pour les autres unités.

Nous avons choisi, pour travailler sur cette démarche, une base commune de connaissances provenant des référentiels EBIOS et ISO 27000, et nous avons pris en compte les PSSI des tutelles (PSSI des établissements d'enseignement supérieur et du CNRS) ainsi que la PSSI de l'État.

Les livrables sont fournis dans un kit « Construction et Déploiement d'une PSSI d'unité », disponible à partir d'un portail (Wiki). Ce kit comporte une méthodologie, des conseils, des documents génériques (présentation type, cartographie des processus…), des outils (support pour entretiens, grille d'analyse des risques...), accompagnés d'une proposition de PSSI générique. Le laboratoire pourra ainsi construire sa PSSI « à la carte », en sélectionnant avec les degrés d'appropriation qu'il souhaitera (du plus générique au plus spécifique), les éléments du kit.

Cette méthodologie est actuellement en application dans 9 laboratoires, et principalement des laboratoires comportant des ZRR, ceux-ci ayant l'obligation de disposer d'une PSSI.

Mots-clefs

PSSI, UMR, ZRR, CSSI, EBIOS, ISO 27000, risque, mesure de sécurité

1 Contexte

Les établissements d'enseignement et de recherche du site grenoblois concernés par les conventions de site (Université Grenoble Alpes, Grenoble INP, Sciences Po Grenoble, Université Savoie Mont-Blanc et CNRS) ont adopté, il y a déjà 8 ans une organisation collégiale de pilotage autour des questions de sécurité de l'information, instituée dans les conventions quinquennales de site. Un comité de pilotage, constitué de représentants des 5 établissements cités (Vice-Président Recherche, Fonctionnaire Sécurité Défense d'université, Responsable Sécurité du Système d'Information et délégué régional du CNRS) se réunit au moins 1 fois par an pour faire un bilan, fixer des objectifs communs et fédérer les unités concernées autour d'outils mutualisés. Une charte d'usage et une charte des administrateurs communes ont ainsi été élaborées et un portail d'information mis en place. Des listes de diffusion et une procédure unique de gestion d'incidents sont également disponibles afin que chaque établissement dispose d'une information homogène et pertinente.

A la demande du comité de pilotage, un chantier de réflexion sur la mise en œuvre de PSSI d'unité a été initié dès 2011 et un groupe de travail s'est constitué autour de cette réflexion, groupe de travail composé de RSSI (UGA, Grenoble INP et CNRS), coordinateurs régionaux du CNRS, et plusieurs chargés de sécurité des systèmes d'informations (CSSI) d'unités. Les trois laboratoires participants (CERMAV[1], TIMA[2], LEPMI[3]) sont représentatifs des thématiques et des organisations de recherche présentes sur le site grenoblois (UPR et UMR des domaines chimie, biologie, physique et informatique).

1. CERMAV : CEntre de Recherches sur les MAcromolécules Végétales UPR 5301
2. TIMA : Techniques de l'Informatique et de la Microélectronique pour l'Architecture des systèmes intégrés – UMR 5159
3. LEPMI : Laboratoire d'Électrochimie et de Physicochimie des Matériaux et des Interfaces – UMR 5279

2 PSSI d'unité

2.1 Objectifs du groupe de travail

Il est souvent difficile d'initier et surtout d'aboutir dans une démarche de mise en œuvre de PSSI d'unité pour un CSSI[4] non accompagné et pas forcément soutenu par sa hiérarchie (souvent non sensibilisée). Face à ce constat, le groupe de travail s'est donc fixé comme objectifs principaux de fournir une méthode, des outils et des éléments « génériques » (sous forme de kit) aux CSSI afin de les accompagner au mieux dans cette démarche. Fort de l'expérience des universités de Grenoble, dans la définition de la « PSSI Générique » des Établissements d'Enseignement Supérieur et de Recherche [1][2], une démarche similaire mais plus souple a été employée, centrée sur une définition qui se veut « exhaustive » du système d'information d'une unité de recherche. Le CSSI, avec le soutien indispensable de sa hiérarchie, pourra ainsi construire la PSSI de son unité à la carte, en piochant (ou non), avec les degrés d'appropriation qu'il souhaitera (du plus générique au plus spécifique), dans les éléments proposés par le kit.

Pour constituer ce kit, les étapes suivantes ont été nécessaires :

- dérouler de bout en bout une démarche de construction de PSSI avec chacun des laboratoires pilotes en parallèle ;
- à chaque étape, en tirer des éléments communs, tant sur la méthode que sur les résultats, qui pourront servir de « modèles » pour les autres unités ;
- intégrer ces éléments dans un kit disponible sous format numérique ;
- présenter la démarche et le kit auprès de l'ensemble des CSSI (réunion, formation).

2.2 Organisation

Le groupe de travail a adopté une organisation autour de réunions régulières, pour faire des points de situation et une restitution annuelle auprès du comité de pilotage.

Une réunion de lancement a été organisée en présence du comité de pilotage et des directeurs d'unité des 3 laboratoires concernés, pour officialiser la démarche.

Chaque CSSI d'unité a fonctionné en binôme avec un partenaire RSSI ou coordinateur CNRS dans les différentes étapes d'exploration et d'identification des risques. Les étapes nécessaires à la constitution d'une PSSI ont donné lieu à une validation par la direction de l'unité :

- identification des processus et personnes référentes à interviewer ;
- réalisation des interviews d'expression des besoins de sécurité ;
- appréciation du risque ;
- choix des mesures de sécurité (établissement de la déclaration d'applicabilité -DdA[5] - selon l'ISO 27001 [3]);
- validation de la PSSI.

Cette organisation a nécessité une base commune et minimale de connaissances :

- formations aux interviews et aux méthodes utilisées (EBIOS [4], ISO 27001…),
- prise en compte des PSSI des tutelles (PSSI des établissements d'enseignement supérieur [5], PSSI CNRS de 2012 [6][7] et PSSI de l'État [8]).

4. CSSI : Chargé de Sécurité du Système d'Information

5. Pour simplifier nous assimilerons la déclaration d'Applicabilité (DdA) de l'ISO 27001, avec la liste des mesures retenues et le plan d'application.

3 Kit de déploiement

3.1 Livrables

Les livrables sont fournis dans un kit « Construction et Déploiement d'une PSSI d'unité » accessible en ligne aux CSSI et comportant :

- une méthodologie, des conseils et explications ;
- des documents génériques : présentation des objectifs de la PSSI d'unité, organisation proposée dans l'unité, cartographie des processus et données de l'unité ;
- des outils :
  - un support pour les entretiens,
  - une grille d'analyse des risques avec son guide d'utilisation,
  - des documents de sensibilisation (CNRS),
  - un comparatif des DdA des laboratoires pilotes ;
- une proposition de PSSI générique en lien avec la PSSI du CNRS et la PSSI de l'État

3.2 Démarche

Le kit PSSI est présenté suivant 2 axes :

- un premier axe qui aborde la construction de la PSSI suivant la logique méthodologique : description des étapes, documents de travail à chaque étape ainsi que les livrables
- le second axe est le mode d'emploi du kit qui permet d'accéder directement à une étape particulière.

La description de la méthode utilisée (voir ci-dessous) est là pour donner un aperçu des différentes étapes de la construction d'une PSSI. Il est nécessaire de prendre le temps de la lire pour bien comprendre ces différentes phases. Ensuite le CSSI peut choisir, après comparaison des données de l'unité avec les données génériques fournies, soit d'adopter telle quelle la PSSI générique, soit de l'adapter aux spécificités de l'unité, soit même de la réévaluer en refaisant tout ou partie de l'analyse de risque.

3.2.1 Description de la méthode

Déroulement de l'élaboration d'une PSSI d'unité et documents PSSI générique associés :

Étape	Documents d'aide	Documents génériques	Livrables
Présentation	Présentation des objectifs de la PSSI d'unité		
Démarrage : prise de décision		Proposition d'organisation	Lancement du projet par la direction Périmètre et enjeux de la PSSI Organisation : comité de sécurité Communication sur le projet

Étape		Documents d'aide	Documents génériques	Livrables
Cartographie des actifs de l'unité			Cartographie générique des processus et données d'un laboratoire	La cartographie du SI de l'unité
Analyse de risque	Critères de sécurité	Échelles employées		Le tableau d'analyse de risque de l'unité La grille expression des besoins de sécurité des processus
	Expression des besoins	Guide de conduite d'entretien Support pour les entretiens	Grille générique remplie	
	Identification des vulnérabilités	Guide d'utilisation du tableau d'analyse de risque		
	Scénarios de menace – niveaux de risques	Guide d'utilisation du tableau d'analyse de risque		
Traitement des risques		Guide de description et d'utilisation de la DdA	DdA générique	La DdA de l'unité
Adoption de la PSSI				Le tableau de bord de mise en œuvre L'adoption de la PSSI par le Conseil de laboratoire L'organisation de management de la sécurité de l'information Communication sur la PSSI

3.2.2 Mode d'emploi

Pour faciliter la lecture, on attribuera au CSSI les différentes tâches, alors qu'il est préférable qu'elles soient réalisées par tout ou partie du groupe de travail de l'unité.

3.2.2.1 Cartographie

Le CSSI compare la cartographie générique à la cartographie du SI de l'unité. S'il ne trouve pas de processus manquant, il convient de passer directement à l'étape suivante. Dans le cas contraire, une adaptation, avec une analyse de risque limitée aux processus manquants sera nécessaire.

La cartographie obtenue devra être validée par le comité de sécurité du laboratoire.

3.2.2.2 Expression des besoins de sécurité

Ici 3 possibilités :

1. Le CSSI n'a que peu de temps à accorder à la PSSI : il adopte les valeurs moyennes des labos témoins, et il passe directement à l'étape suivante.
2. Le CSSI a un peu de temps ou l'unité a des processus particuliers : il adopte automatiquement les valeurs communes, et il ne se pose des questions que pour les valeurs qu'il estime différentes, ou pour les nouveaux processus ; pour cela il fait des interviews rapides des divers responsables métiers concernés.
3. Le CSSI a plus de temps ou il est perfectionniste : il vérifie l'ensemble des valeurs fournies avec des interviews rapides des divers responsables métiers concernés.

La méthode choisie devra être validée par le comité de sécurité du laboratoire.

3.2.2.3 Analyse de risque

Ici 2 possibilités pour mener l'analyse de risque :

1. Le laboratoire ne présente pas de spécificités (locaux, environnement, matériels, type de recherche…) qui pourraient amener des vulnérabilités ou des menaces particulières : le CSSI adopte les données génériques et passe directement au point suivant.
2. Le laboratoire a des processus très sensibles, des spécificités (locaux, environnement, matériels…), il a déjà été soumis à des événements de sécurités importants ou au contraire, il ne présente que peu de vulnérabilités : le CSSI révise tout ou partie des menaces et vulnérabilités proposées.

Ces choix devront être validés par le comité de sécurité du laboratoire.

3.2.2.4 Traitement de risques

Une fois l'analyse de risque terminée, il va falloir définir le plan de traitement des risques. Chaque combinaison de besoins de sécurité, de niveau de vulnérabilités, de vraisemblance de menaces donne un niveau à un scénario de risque. Là encore pour l'aider à faire ce choix, le CSSI dispose de la déclaration d'applicabilité (DdA) générique issue de celles des laboratoires pilotes. Le plan de traitement des risques devra être établi en fonction de la criticité des mesures, de la facilité à les mettre en œuvre (organisation, technicité), ou de leur coût.

Le plan de traitement des risques devra être validé par le comité de sécurité du laboratoire.

3.2.2.5 La PSSI

La PSSI est terminée, puisque l'on dispose de la description de l'organisation mise en place, des mesures que l'on a retenu (DdA), et du plan de traitement des risques L'ensemble devra être validé par le conseil de laboratoire.

Il ne reste plus qu'à mettre en place un tableau de bord de mise en œuvre des mesures et de le faire évoluer dans le temps.

Au moins une fois par an, une revue de la PSSI devra être effectuée par le comité de sécurité du laboratoire en prenant en compte :

- la difficulté de mise en œuvre des mesures,
- les nouvelles menaces ou vulnérabilités à prendre en compte,
- l'efficacité des mesures en place (incidents, tests d'intrusion...),
- la modification du plan de traitement des risques,
- le changement du périmètre physique ou fonctionnel,
- les nouvelles réglementations...

et bien sûr les modifications qui en découlent devront être adoptées par le conseil de laboratoire.

3.3 Retour d'expérience

La démarche a pris plus de 3 ans car elle s'est déroulée de façon asynchrone avec beaucoup de délais d'attente à chaque phase. Certains délais sont imputables au temps nécessaire à la prise en compte de la démarche PSSI dans chaque laboratoire : mise à l'ordre du jour du conseil de laboratoire ou d'une assemblée générale, intégration dans le planning du CSSI et des métiers interviewés. D'autres délais sont imputables au temps de synthèse commun pour la production des éléments génériques : démultiplication des restitutions et échanges, rapprochement des résultats pour identifier les éléments communs et construction du kit une fois que tous les laboratoires ont achevé chaque étape.

Pour chaque laboratoire, la démarche a été très profitable à plusieurs titres :

- les nombreux échanges en interne avec les métiers ont permis une meilleure connaissance de l'activité des personnels par le CSSI ;
- ces échanges ont constitué une sensibilisation à la sécurité ;
- les entretiens en binôme ont permis de conforter le CSSI dans son rôle, de montrer l'intérêt des tutelles pour le laboratoire, de limiter les discussions hors sujet et enfin de profiter de l'expérience de l'accompagnateur du CSSI, celui-ci ayant souvent un angle de vue différent et complémentaire ;
- les directions des unités concernées ont pris conscience de l'importance du sujet.

3.4 Utilisation actuelle

Cette méthodologie est actuellement en application dans 9 nouveaux laboratoires. Plusieurs comportent des ZRR, et se voient dans l'obligation de disposer d'une PSSI.

Tous perçoivent le kit comme une aide qui facilitera leur projet. Ces laboratoires bénéficient, comme les unités pilotes, de l'assistance des RSSI et CRSSI des tutelles qui ont conduit la démarche initiale.

Les CSSI de ces 9 unités se sont appropriés la démarche, et commencent à l'utiliser : description de la démarche auprès de la direction, utilisation de la présentation générique en assemblées générales, vérification de la cartographie proposée, etc.

Contrairement à la phase pilote, chaque laboratoire est maître de son calendrier.

4 Conclusion

Depuis 2011 le panorama des PSSI des tutelles a changé, en particulier avec la publication de la PSSI de l'État. La plupart des tutelles disposent désormais de leur propre PSSI et la proposent telle quelle à leurs composantes, ce qui pose problème aux unités mixtes.

Construire sa PSSI d'unité présente alors des avantages qui méritent d'être examinés :

- la PSSI adoptée fait la synthèse des PSSI des tutelles du point de vue du laboratoire ;
- cela permet la mise en adéquation avec les risques réels et les ressources du laboratoire ;
- cela contribue aussi à une sensibilisation et une appropriation plus efficace par les membres du laboratoire qui se sont impliqués dans la démarche au lieu d'avoir le sentiment de subir les mesures adoptées ;
- cela légitimise le CSSI dans son rôle vis à vis de la direction et vis à vis de ses collègues.

Enfin et plus spécifiquement, cette démarche favorise grandement l'identification et la compréhension de la circulation des données sensibles dans les différents processus métiers de l'unité. A l'aube de la mise en application du nouveau règlement européen sur les données personnelles (RGPD), il parait évident que la simple application des PSSI d'établissement et/ou institutionnelle ne sera pas suffisante pour garantir la conformité aux dispositions légales. Rien ne remplacera la connaissance terrain pour mettre en place une analyse de risque pertinente sur les données personnelles.

Un tel projet reste cependant complexe. Il a été conduit exhaustivement sur trois laboratoires pilotes du site grenoblois. Les laboratoires qui commencent à utiliser le kit en perçoivent déjà les bénéfices. Les autres laboratoires du site disposent à présent du kit et doivent se mettre en ordre de marche.

Bibliographie

[1] **Dominique Launay, Jean-Paul Le Guigner**. Projet de PSSI générique pour les établissements d'enseignement supérieur. Dans Actes du congrès JRES2009, Nantes, Décembre 2009. https://2009.jres.org/planning_files/summary/html/83.htm

[2] **Bernard Martinet, Annie Cobalto, Dominique Launay, Roger Negaret.** Démarche PSSI générique : retour d'expérience d'établissements pilotes. Dans Actes du congrès JRES2011, Toulouse, Novembre 2011. https://2011.jres.org/archives/101/index.htm

[3] **ISO.** Famille ISO/IEC 27000 - Systèmes de gestion de sécurité de l'information.

[4] **ANSSI**. EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité. [En ligne] https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite

[5] **GT-PSSI/CRU.** PSSI générique pour les établissements d'enseignement supérieur et de recherche. [En ligne] https://services.renater.fr/ssi/rssi/pssi/index

[6] **CNRS**. Politique Générale de Sécurité de l'Information du CNRS [En ligne]. https://extra.core-cloud.net/collaborations/RSSI-CNRS/SitePages/Accueil.aspx

[7] **CNRS.** Politique Sécurité des Systèmes d'Information opérationnelle applicable aux laboratoires du CNRS. [En ligne]. https://extra.core-cloud.net/collaborations/RSSI-CNRS/SitePages/Accueil.aspx

[8] **ANSSI.** La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE). ANSSI. [En ligne] 17 Juillet 2014. https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/.