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

Bernard Martinet (orateur)
Annie Cobalto
Dominique Launay
Roger Négaret

Plan

- Rappel sur le projet PSSI générique
- Le référentiel générique
- Synthèse des 7 projets établissements
- Focus sur 3 établissements

Le projet PSSI générique

- Constitution des équipes projet en établissement
- Élaboration d'un référentiel commun
- Entretiens au sein de chaque établissement
  - contexte, besoins de sécurité,vulnérabilités
- Sur trois périmètres
  - gestion, pédagogie et enseignement, recherche

Le projet PSSI générique (2)

- Consolidation des données par la société Fidens
- Identification des risques (scénarios de menace)
- Sélection des mesures adaptées et rédaction des règles de la PSSI et des autres documents du référentiel
- Livraison de la PSSI propre à chaque établissement

Le référentiel générique

- Une politique de management de la sécurité de l'information (PMSI)
- Une politique de sécurité des systèmes d'information (PSSI)
- Une politique générale de la sécurité des systèmes d'information (PGSSI)
- Une matrice de correspondance des règles et mesures
- Une déclaration d'applicabilité type (mise en œuvre)
- Un plan d'action type pour l'implémentation d'un SMSI

Synthèse des 7 projets en établissement

- Les établissements
  - Université de la Méditerranée (Aix-Marseille Université)
  - Université de Bordeaux 1
  - Université de Limoges
  - Université de Nancy (PRES Université de Lorraine)
  - Université de Rennes 1
  - Université de Grenoble (PRES)
  - Réseau Universitaire Numérique Normand (UNR)

Synthèse : organisation projet

Pour chaque établissement

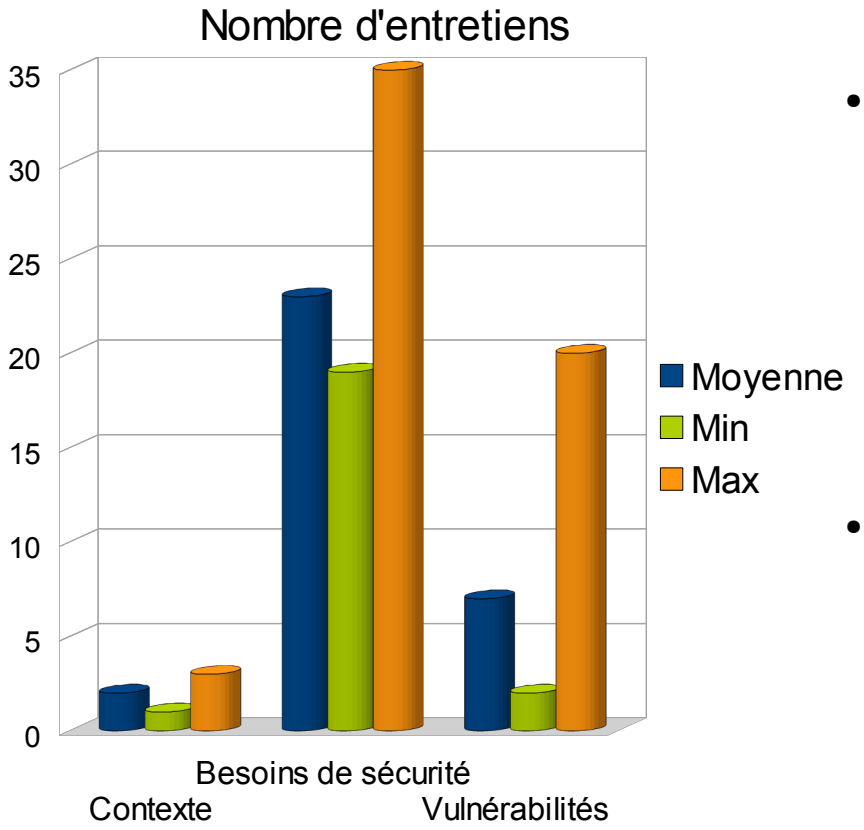
- **Équipe projet (3 à 6 personnes)**
  - Entretiens
  - Cartographie
  - Validation
  - ...
- **Comité de pilotage**
  - Spécifique ou
  - Basé sur un comité existant

Structure classique mais indispensable à la réussite du projet

Synthèse : Analyse de Risque

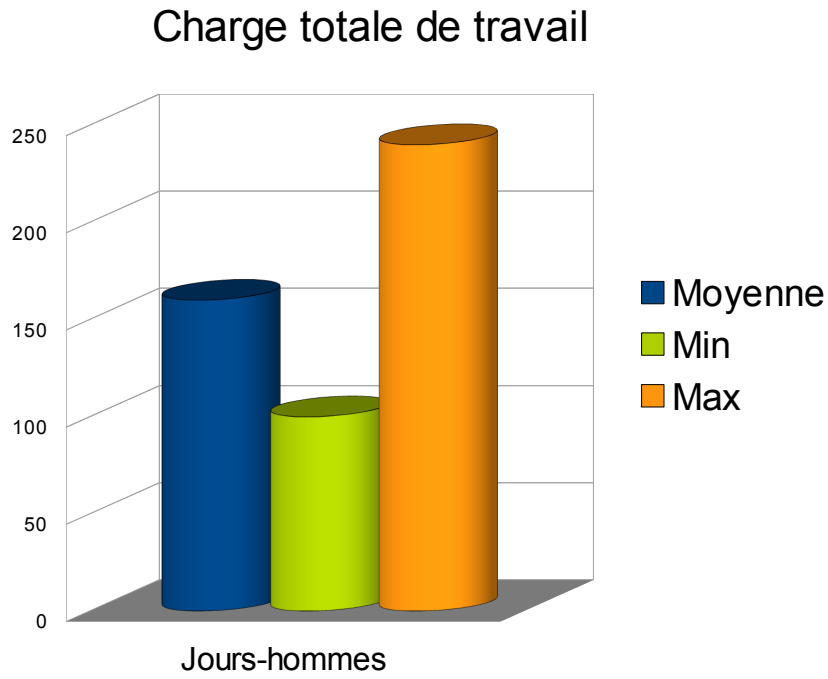
- Durée : 1 à 4 mois (2,5 en moyenne) pour entretiens, menaces, risques
- Les entretiens
  - durée 1h à 2h (1h30 en moyenne)
  - ½ à 1 journée avec préparation, analyse, mise en forme, validation
  - réalisés la plupart du temps en tandem au niveau de l'équipe projet

Synthèse : Entretiens



- Phase essentielle de l'analyse de risques :
  - rencontre des acteurs au plus haut niveau de la gouvernance
  - l'interlocuteur doit être choisi en fonction de l'entretien (contexte, besoins de sécurité, vulnérabilités)
- Occasion de sensibiliser les acteurs à la SSI dans leur métier

Synthèse : Charge de travail



- Non compris :
  - temps passé dans le groupe de travail national
  - temps de formation
  - temps de validation final des documents
- Fonction de :
  - structure de l'établissement analysé
  - périmètre retenu
  - finesse de l'analyse de risques produite
  - détail de la PSSI

Synthèse : les comités SSI

Comité de pilotage stratégique	• Valide et gère la PSSI • 1 réunion par an (préconisation générique)
Comité de sécurité opérationnel	• Évolution de la PSSI, analyse et traitement des risques, processus de suivi • 3 à 4 réunions par an (préconisation générique)
Comité de liaison	• Relais des décisions de sécurité vers les composantes, gestion des incidents • Réunions régulières

Il est souvent plus simple d'affecter ces rôles à des comités déjà existants

Focus sur 3 établissements

- Une université : l'Université de Rennes 1
- Un Pôle de Recherche et d'Enseignement Supérieur : le PRES Université de Grenoble (4 universités, 1 école d'ingénieurs et 1 institut d'études politiques)
- Une Université Numérique en Région : l'UNR RUNN - Réseau Universitaire Numérique Normand (3 universités et 2 écoles d'ingénieurs)

Organisation projet

Equipe projets		
	Composition	**Effectifs**
Rennes	RSSI, RSSI adjoint , responsable de cellule de proximité, un CSSI CNRS + l'animateur du groupe projet national	5
Grenoble	4 RSSI (ou adjoints) issus de 4 des 6 établissements du PRES	4
RUNN	3 RSSI (ou adjoints) et l'assistant du groupe de travail SSI du RUNN	4

La décision de participer au projet PSSI générique a été prise à un niveau politique dans les trois établissements.

Organisation projet (2)

Comité de pilotage projet			
	Comité existant	Composition	Effectif
Rennes	oui	Président, plusieurs Vice-Présidents, la Directrice Générale des Services, le Directeur du CRI, le RSSI	9
Grenoble	oui	Les DGS et les VP SI des 6 établissements, Le Directeur du PRES, les 2 coordinateurs SSI inter-universitaire et le CIL	15
RUNN	non	2 VP et le chef de projet RUNN, les 5 DGS, un DSI, un ingénieur Hygiène et Sécurité, un CIL, un représentant du CNRS et l'équipe projet	16

Les entretiens

	Nombre	Durée totale
Rennes	25	1,5 mois
Grenoble	24	2 mois
RUNN	28 + 11	2 mois

Personnes interviewées

- DGS, VP
- Chefs de services ou responsables métiers (RH, Scolarité, Finances, H&S...)
- Directeurs d'UFR, Instituts, Écoles, Laboratoires...
- RSSI, DSI, ASR
- Responsables projets

Traitement des livrables

- La PMSI
  - Adaptée aux structures en place dans les 3 cas
- La PSSI de Rennes, 3 volets
  - PSSI - Principes généraux : issu de la PGSSI générique
  - PSSI - Règles : toutes les règles ont été révisées par un comité d'experts selon les domaines abordés
  - PSSI - Documents d'application : devra contenir tous les documents auxquels il est fait référence dans les règles

Traitement des livrables (2)

- La PSSI de Grenoble
  - La PGSSI est retenue comme PSSI. Nous restons 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.
  - La PSSI détaillée sert de base à la rédaction des documents annexes et à la mise en œuvre des mesures

Traitement des livrables (3)

- La PSSI du RUNN
  - c'est le document de PSSI générique détaillée, adapté au contexte local
  - certaines mesures font référence à des documents d'application plus techniques (en cours d'écriture)

Les différents comités SSI

Comité de pilotage stratégique			
	Comité existant	Composition	Effectif
Rennes	oui	le comité stratégique du SI : Président, DGS, VP finance, 2 VP, DSI	6
Grenoble	variable suivant étab.	Pilotage stratégique du domaine de chaque établissement. Pour le périmètre recherche il existe un comité de coordination SSI Universités-CNRS	variable 15
RUNN	non	Pour chaque établissement : Président ou directeur, 1 personne désignée (FSD, DGS ou DSI), le RSSI + le chef de projet RUNN + un représentant du CNRS	17

Les différents comités SSI

Comité de sécurité opérationnel			
	Comité existant	Composition	Effectif
Rennes	non	RSSI, RSSI adjoints, CIL, un représentant du service juridique, représentants de la DSI, experts invités	5 à 10
Grenoble	Oui concatenation de comités existants	Pour chaque établissement : DGS, VP SI, DSI et RSSI Directeur du PRES + Directeur service informatique mutualisé	25
RUNN	Oui (GT SSI RUNN)	Pour chaque établissement : RSSI et RSSI adjoints CRSSI du CNRS 1 assistant du groupe de travail	17

Les différents comités SSI

Comité de liaison			
	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	non	Comité de liaison au niveau de chaque établissement Pour l'Université de Caen comité de liaison composé des chargés de la SSI dans les composantes et unités de recherche (36 nommés à ce jour)	36 à Caen

Plans d'action

Rennes :

- mise en œuvre en attente de création du comité de sécurité opérationnel
- des analyses de risques complémentaires devront être menées sur des périmètres précis
- une étude sur la gestion de l'authentification est en cours

Plans d'action (2)

Grenoble :

- réunion du comité de liaison ½ journée par semaine avec ou non présence d'experts métiers
- 13 chantiers PSSI, regroupés autour d'axes fédérateurs ou de métiers, ont été définis sur un délai de 18 mois
  - 4 reposant essentiellement sur les composantes informatiques (ASR, DSI + RSSI), sont en cours
  - 9 nécessitant le concours d'experts métiers sont en attente des plans de communications

Plans d'action (3)

RUNN :

- réunions mensuelles pour le comité de sécurité opérationnel
- sur une première période de 15 mois
  - inventaire complet des biens du RUNN
  - sensibilisation des acteurs dans les établissements
  - déclinaison de la PSSI dans chaque établissement
  - rédaction des documents d'application
  - mise en œuvre de la gestion de la sécurité : tableau de bord, indicateurs...

Difficultés et apports

	Les difficultés	Les apports
Rennes	• Étendue du périmètre • Appréciation exhaustive du risque à l'échelle d'un établissement difficile à appréhender.	• Un document listant de manière exhaustive tous les sujets de sécurité • Mise en place des comités
Grenoble	• Modification du périmètre en cours de projet • Structure multi-établissement qui ralentit les phases de décision	• La mise en place d'une gestion de la SSI, avec prise en compte des besoins • Volonté affichée par la gouvernance d'avancer sur ce domaine.
RUNN	• Définition du contexte et du périmètre • Difficulté d'appropriation de la PSSI par les directions des établissements • Inquiétude des ASR • Charge de travail	• Dynamique et émulation inter-établissements • Prise de conscience des risques et des responsabilités de chacun • Reconnaissance des RSSI • Mise en place d'une base SMSI

Conclusion

- Une PSSI pour une Université voire un PRES est possible !
- Tâche ardue mais faisable avec une organisation adaptée et un soutien de la gouvernance (1 équipe projet + 1 pilotage)
- Importance du contexte ; les entretiens sont un moment privilégié de sensibilisation
- Le pragmatisme est de mise !
- Vous êtes prêt pour votre 1er tour de roue 27001

Tous les documents du projet sont sur l'intranet des RSSI !