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

JRES 2005 marseille

Groupe de travail CAPSEC

- Composition
  - 5 coordinateurs sécurité CNRS (informaticiens impliqués dans la sécurité)
  - 1 conseiller de la DCSSI
- Validé par l'UREC
- Objectif : rédiger des documents génériques pour aider les entités CNRS à définir la Politique de Sécurité de leur Système d'Information (PSSI)

Plan

- Contexte
- Pourquoi une PSSI ?
- Démarche utilisée et Documents élaborés
- Quelles étapes suivre ?
- Évolution

Contexte

- Autonomie des 1300 entités du CNRS
- Complexité du Système d'Information (SI) (nomadisme, nombre croissant de logiciels, et d'utilisateurs) sur des réseaux partagés
- Existence de solutions techniques

→ Nécessité d'une approche globale et méthodique pour sécuriser le SI en concertation avec les utilisateurs

= Objectif du groupe de travail CAPSEC

Pourquoi une PSSI ?

- Sécuriser les résultats de recherche

  Ex : protéger brevets et articles avant leur publication

- Prendre conscience des menaces pesant sur le SI

  Ex : mauvaise gestion des accès aux données

  → divulgation de documents confidentiels
  → perte d'un contrat industriel

- Organiser procédures de reprise des services

  Ex : procédures à suivre en cas de dysfonctionnement du serveur de courrier

Plan

- Contexte
- Pourquoi une PSSI ?
- Démarche utilisée et Documents élaborés
- Quelles étapes suivre ?
- Évolution

Démarche

Utilisation d'une méthode et d'un guide de la DCSSI

- EBIOS « Expression des Besoins et Identification des Objectifs de Sécurité »
  = méthode de gestion des risques
- Guide PSSI
  = liste des principes de sécurité

Documents élaborés

- À partir du logiciel EBIOS
  - Étude EBIOS générique ; Note de stratégie
  - Fiche enquête (enjeux, données et services à sécuriser)
  - Liste des menaces retenues
- À partir du guide PSSI
  - Principes de sécurité
  - Règles de sécurité

→ Pour récupérer ces documents :

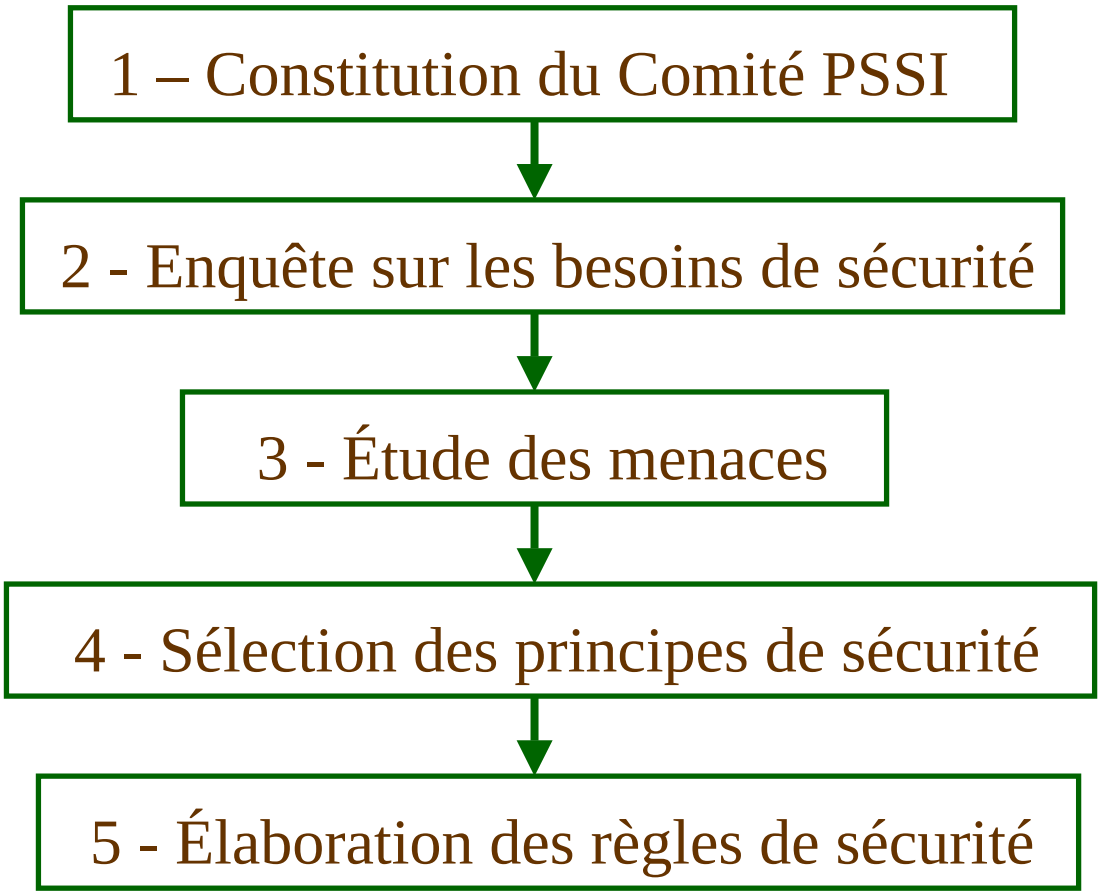
CNRS : https://www.urec.cnrs.fr/securite/corres-secu/CAPSEC

Autres : sur demande à capsec@urec.cnrs.fr

Plan

- Contexte
- Pourquoi une PSSI ?
- Démarche utilisée et Documents élaborés
- Quelles étapes suivre ?
- Évolution

Quelles étapes suivre ?



Étape 1 – Constitution du Comité PSSI

- Rôle du Comité PSSI : étudier et proposer la PSSI de l'entité
- Membres :
  - Direction
  - Représentants des utilisateurs
    - Responsables des équipes de recherche
    - Responsables des services
  - Correspondant sécurité ou ASR
  - Collaborateurs extérieurs (CRI, …)

Étape 1 – Constitution du Comité PSSI

- Important

  Participants doivent être représentatifs

- Pièges à éviter

  Nombre de participants trop élevé (entre 5 et 10 personnes)

- Difficulté rencontrée

  Motiver la participation à ce comité

Étape 1 – Exemples Comité PSSI

Membres / Entité	ATILF	CRPP	Observatoire de Besançon	LORIA
Directeur ou représentant	1	1	1	1
Correspondant sécurité ou ASR	1	1	1	1
Représentants des équipes de recherche	2	5	3	3
Représentants des services	1	2		1

Étape 2 – Enquête sur les besoins de sécurité

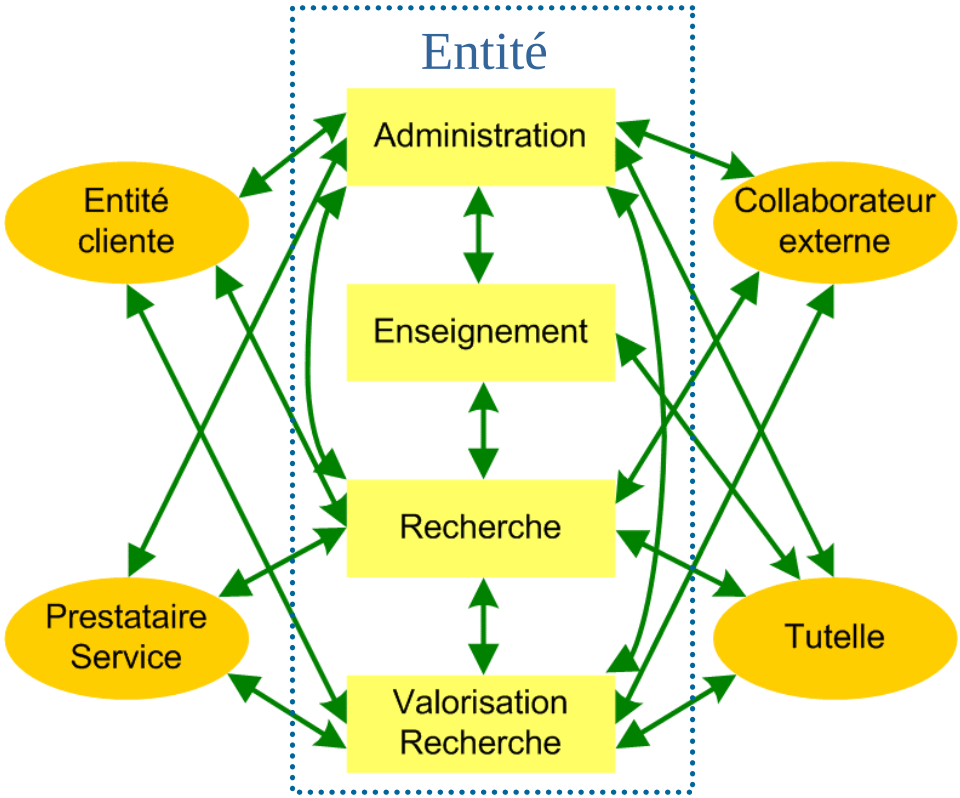
- Objectif : Le comité PSSI doit répondre aux questions :
  - Données utilisées ? Localisation de ces données ?
  - Émetteurs et destinataires de ces données ?
  - Niveau de sécurité sur ces données et fonctions ?
- …Tout en connaissant les enjeux :
  - Financiers (perte de contrats)
  - Politiques (image de marque, crédibilité)
  - Techniques (conservation des savoir-faire)
- Distribution de l'enquête au Comité PSSI, responsables d'équipe et de service, utilisateurs

Étape 2 – Enquête sur les besoins de sécurité

- Exemples de données
  - Contrats confidentiels
  - Savoir-faire
  - Enseignement (notes et sujets d'examen)
  - …
- Exemples de fonctions
  - Communication (Ex : Serveur de courrier)
  - Publications (Ex : Serveur web)
  - …

Étape 2 – Enquête sur les besoins de sécurité – Les acteurs du SI

Émetteurs et destinataires des données ? Localisation ?



Étape 2 – Enquête sur les besoins de sécurité – Échelle des besoins

Besoin de sécurité	Disponibilité	Intégrité	Confidentialité
0	Sans conséquence	Sans conséquence	Sans conséquence
1	Long terme (8h→1 semaine)	Gène de fonctionnement	Gène de fonctionnement
2	Moyen terme (2h→8h)	Conséquences dommageables	Conséquences dommageables
3	Court terme (Temps réel→2h)	Conséquences graves	Conséquences graves

Étape 2 – Enquête sur les besoins de sécurité – Exemple

Type de donnée	Critère de sécurité	Niveau de sécurité de l'entité	Valeur indicative (CAPSEC)
Contrats industriels	Confidentialité		2
	Disponibilité		1
	Intégrité		2
Expérimentales	Confidentialité		1
	Disponibilité		2
	Intégrité		2

Étape 2 – Enquête sur les besoins de sécurité – Conclusion

Le Comité PSSI rédige la synthèse des réponses aux enquêtes

Étape 2 – Enquête sur les besoins de sécurité – Bilan (1)

- Bénéfices / utilisateur
  - Les utilisateurs prennent en main leurs besoins de sécurité informatique
  - Les utilisateurs prennent conscience de l'importance de leurs données et des menaces
  - Meilleure localisation des données

    ex : les boites aux lettres sur les ordinateurs portables
- Bénéfices / entité

  ➡ Meilleure sensibilisation à la sécurité informatique
  - Connaissance réelle des besoins de sécurité

Étape 2 – Enquête sur les besoins de sécurité – Bilan (2)

- Difficultés rencontrées
  - Sujet nouveau
    - → explication des termes de la fiche d'enquête aux membres du Comité PSSI (Ex : intégrité, gestion des risques)
    - → exemples concrets de menaces sur les données
  - Temps important à consacrer à l'accompagnement de l'enquête

Étape 3 – Étude des menaces

- Hypothèse de travail : personnel ayant accepté la charte informatique est de confiance
- Pour chaque menace :
  - Qui prend en compte cette menace ?
  - Origine de la menace ? (environnementale, humaine ou naturelle)
  - Cause de la menace ? (délibérée ou accidentelle)
  - Probabilité d'apparition de la menace ?

  → Menace retenue ?

Étape 3 – Étude des menaces

- Exemples de menaces
  - Incendie
    - À étudier par la Commission Hygiène et Sécurité
  - Écoute passive
    - Comment ? Installation par jeu de programmes permettant d'écouter ce qui passe sur le réseau interne
    - Qui ? Pirate, personnel temporaire, visiteurs
  - Piégeage du logiciel (vers, virus, etc…)

Étape 3 – Étude des menaces

- Possibilité d'ajout de menaces spécifiques

  Ex : Vol de l'antériorité de l'idée
- IMPORTANT : si une menace n'est pas retenue, les utilisateurs doivent être informés des risques encourus

Étape 4 – Comment aborder les principes de sécurité ?

- Objectif : fixer les orientations et caractéristiques de la PSSI
- À partir de quoi ?
  - Synthèse des fiches d'enquêtes
  - Étude des menaces
  - Référentiel des principes CAPSEC

Étape 4 – Comment aborder les principes de sécurité ?

- 2 types de principes
  - Principes obligatoires imposés par le schéma directeur

    Ex : « Responsabilités générales pour la SSI de l'organisme »
  - Principes à sélectionner par le Comité PSSI

    Ex : « Cloisonnement des postes sensibles »

Étape 4 – Comment aborder les principes de sécurité ?

- Exemple : est-ce que le principe « Cloisonnement des postes sensibles » est retenu ?
  - Modalité d'application du principe

    Séparation dans un réseau dédié des ordinateurs comportant des données liées à des contrats industriels avec confidentialité forte
  - Critères de sélection
    - Coût financier ?
    - Temps passé par le service informatique ?
    - Contraintes pour les utilisateurs ?

Étape 4 – Comment aborder les principes de sécurité ?

- Conclusion de cette étape :

  Comité PSSI soumet les principes aux instances décisionnelles (conseil de laboratoire, conseil d'administration…)

- Piège à éviter :

  Vouloir appliquer le même niveau de sécurité à tout le laboratoire

Étape 5 – Comment appliquer les principes de sécurité ?

- Objectif : élaboration des règles de sécurité
- Le correspondant sécurité ou l'ASR détermine procédures et solutions techniques pour chaque principe retenu
- Ex : pour le principe « Cloisonnement des postes sensibles »

  Un vlan pour les utilisateurs travaillant sur des contrats industriels avec confidentialité forte

Bilan dans les laboratoires pilotes

Étapes / Entités	ATILF	CRPP	Observatoire de Besançon	LORIA
Constitution du comité PSSI	✓	✓	✓	✓
Enquête sur les besoins de sécurité	✓	✓	✓	✓
Étude des menaces	✓	✓	✓	EN COURS
Sélection des principes de sécurité	✓	EN COURS	EN COURS	EN COURS
Élaboration des règles à appliquer	EN COURS			

Temps total passé par le correspondant sécurité ou l'ASR ~ 8 jours

Extension de la méthode

- Extension aux universités
  - méthode utilisée à l'université de Franche-Comté
  - à l'étude au CRU
- Extension aux entités d'enseignement supérieur et de recherche

Évolution

- Cohérence avec le Schéma Directeur de l'organisme ou l'établissement pour un déploiement généralisé
- Tableaux de bord : permettent de suivre toutes les actions liées à la Sécurité du Système d'Information
  - Couverture des risques
  - Qualité de la sécurité
  - Suivi des alertes
  - …