ANSSI.lu

Agence nationale de la sécurité des systèmes d'information Luxembourg

La Politique de sécurité de l'information de l'État Luxembourgeois

Jerry Caye, ANSSI

ADaCoR

21 avril 2016

Plan de la présentation

La volonté politique de promouvoir la cybersécurité

- Historique des actions.
- Organisation générale (AGD du 10 février 2015).
- Les missions de l'ANSSI.
- Feuille de route.

La sécurité des SI

- Nécessité d'implémentation d'une politique de sécurité de l'information.

La PSI-LU

- La politique de sécurité de l'information de l'État luxembourgeois.
- Les dix principes de la PSI-LU.
- Les politiques générales par domaine.

Le futur SMSI de l'Etat (PSI-SMSI)

- Le système de management de la sécurité de l'information.

Quand implémenter ?

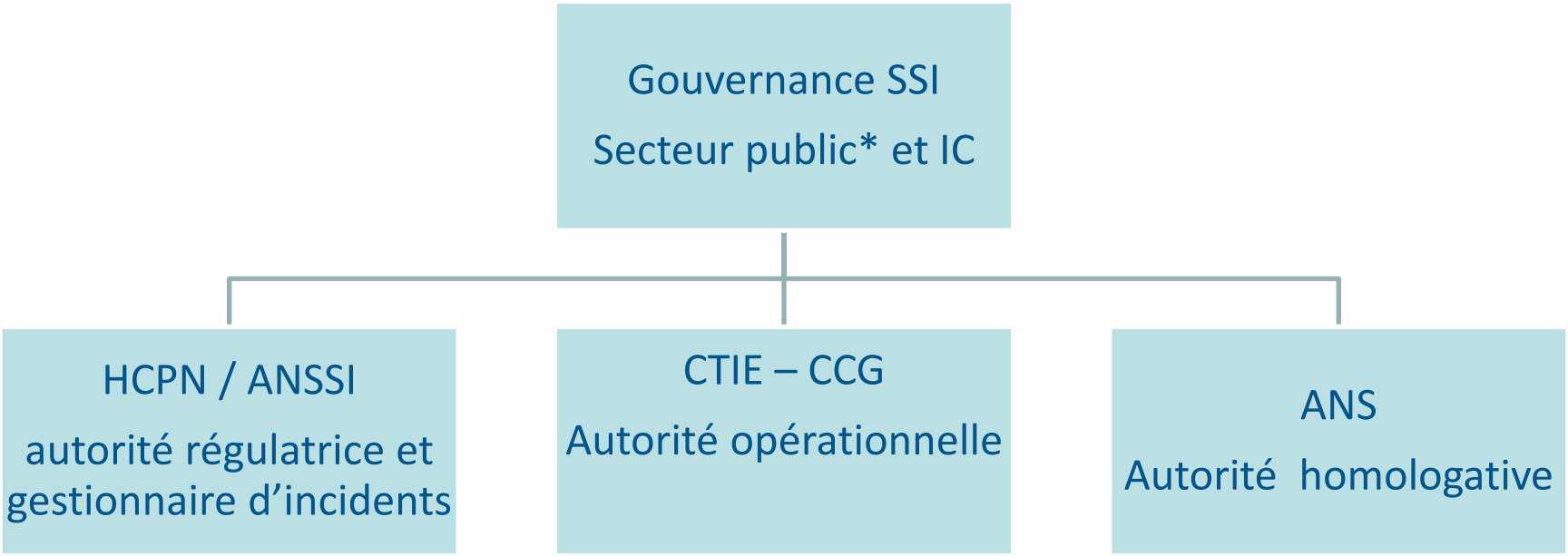
- Étapes d'implémentation pour les entités de l'État.
- Modèle d'organisation d'une implémentation.

La volonté politique

Historique des actions

- Développement d'une stratégie nationale en matière de cybersécurité en 2012 se basant sur cinq axes.
- Version II de cette stratégie début 2015. Protection des acteurs publics et privés contre les cybermenaces en définissant sept objectifs et les plans d'action y relatifs. Mise en œuvre de cette nouvelle stratégie d'ici fin 2017.
- Arrêté grand-ducal du 10 février 2015 portant création d'une agence nationale de la sécurité des systèmes d'information (ANSSI).

Organisation Générale (AGD)



* à l'exclusion des communes

IC: Infrastructures Critiques

Missions ANSSI 1/2

- Le HCPN fait fonction d'ANSSI.

L'ANSSI a pour missions :

- de définir les politiques et lignes directrices en matière de la sécurité de l'information (classifiée et non-classifiée) et d'en surveiller l'efficacité et la pertinence.
- de veiller à ce que les mesures concernant la sécurité des systèmes d'informations soient mises en place et que leur application soit garantie.
- de certifier les moyens de traitement de l'information non classifiée (systèmes, services, infrastructures, ou locaux les abritant).

Missions ANSSI 2/2

L'ANSSI a pour missions :

- d'assurer la fonction de CERT national et gouvernemental.
- de coordonner la formation à la sécurité de l'information classifiée et non-classifiée.
- de veiller à ce que les utilisateurs soient sensibilisés de façon adéquate aux risques spécifiques liés à l'utilisation des systèmes de communication et d'information; notamment aux risques en relation avec les attaques électroniques.
- d'assurer la fonction d'autorité Tempest.
- d'assurer la fonction d'autorité d'agrément cryptographique.

ANSSI – feuille de route

Mise en place de l'ANSSI - Accords de coopération - Création structure ANSSI - Recrutement - Préparation consultance	Février – Juin 2015
Politique de sécurité – régulation (par le recours à des consultants externes)	2e semestre 2015
Consultation et acceptation	Décembre 2015 – Avril 2016

Nécessité d'implémentation d'une politique de sécurité de l'information

Les menaces

- Dommages physiques et catastrophes naturelles.
- Compromission des informations et compromission des fonctions.
- Défaillances techniques, accès et manipulations non autorisés.

L'impact

- Perte de réputation et de crédibilité.
- Indisponibilité.
- Coûts importants de rétablissement d'un mode de fonctionnement normal.

Nécessité d'implémentation d'une politique de sécurité de l'information

Augmentation et évolution des menaces

- Menaces externes (spoofing, ransomware, DDoS, attaque de l'homme du milieu, phishing, intrusion, ...).
- Menaces internes (vol ou perte d'un support amovible/équipement mobile, social engineering, diffusion en ligne de documents confidentiels ou divulgation,...).

La mise en place de mesures techniques n'est pas suffisante, il faut implémenter une politique de sécurité de l'information et élaborer un système de management (définition des responsabilités, procédures et plans d'actions (préventives et réactives), revues périodiques, sensibilisations).

Conclusion: les mesures de sécurité et procédures en place doivent être formalisées en vue d'une implémentation d'une politique de sécurité selon les normes ISO 2700x.

Nécessité d'implémentation d'une politique de sécurité de l'information

Sceptique ?

- Une politique/culture de la sécurité de l'information est-elle en place ?
- Les responsabilités au niveau de la sécurité sont-elles clairement définies et attribuées ?
- Un programme de sensibilisation des utilisateurs est-il appliqué ?
- Une analyse des risques récente a-t-elle été réalisée et documentée ?
- Les plans d'action sont-ils établis et respectés ?
- Connaissez-vous tous vos actifs (« assets ») et leurs valeurs ?
- Quelles consignes à suivre en cas de panne ou de crise ?
- Qui peut s'approcher physiquement de vos actifs à protéger ?
- …

La politique de sécurité de l'information de l'État luxembourgeois

Démarche

- Développement de la politique de sécurité avec le consultant externe itrust consulting.
- Une large consultation a été menée avec les régulateurs et partenaires comme:
  - ILR, CSSF, ILNAS et CNPD.
  - SMILE G.I.E., CTIE, l'ANS et le GovCert.
  - Commissaire du gouvernement à la protection des banques de données de l'État.
- Une lettre circulaire et un questionnaire ont été adressés aux entités étatiques afin d'évaluer le niveau de maturité (75% de feed-back).

Objectifs de la politique de sécurité

- Décrire les objectifs généraux et les principes de sécurité.
- Assurer que les meilleures pratiques soient utilisées afin de protéger les informations que les entités de l'État luxembourgeois traitent.

La politique de sécurité de l'information de l'État luxembourgeois

Champ d'application

- L'ensemble des départements ministériels, administrations et services de l'État luxembourgeois.
- Opérateurs d'infrastructures critiques (après mise en vigueur de la loi portant création du Haut-Commissariat à la Protection Nationale).
- Exclusion: le pouvoir législatif et le pouvoir judiciaire, les administrations communales et les établissements publics.

Disposition transitoire

Le champ d'application de la présente version est limité au CTIE et aux entités qui se portent volontaires pour démarrer la mise en application de cette politique de sécurité. Une évaluation auprès de ces entités permettra de réviser ces exigences et proposer un plan de mise en application pour toutes les entités pour début 2017.

Les dix principes de la PSI-LU

1. Une sécurité bien comprise (programme de sensibilisation).
2. Le respect des normes, des contrats et des lois.
3. Analyse et gestion du risque (afin de sélectionner les mesures de sécurité).
4. Planification, quantification et identification des Ressources.
5. Un développement continu vers l'excellence (changement continuel de l'environnement de gestion des informations).
6. Une sécurité intégrée et transversale; elle fait partie intégrante de toute l'activité de l'État (gestion des projets, des processus et des activités quotidiennes).
7. Communication et travail d'équipe (aide mutuelle dans la réalisation des objectifs de sécurité).
8. Contrôle et sous-traitance (opérateurs et prestataires de confiance).
9. Respect des objectifs et règles de la PSI-LU et traçabilité des activités et décisions concernant le SMSI.
10. Politique et culture de sécurité.

Les politiques générales par domaine (1/2)

Id.	Acronyme	Nom du domaine ou nom de la politique de sécurité	Commentaire
0.0	PSI-LU	**Politique générale**	Politique de sécurité de l'Etat
1-0	PSI-SMSI	**Système de gestion de la sécurité de l'information**	Est l'outil de gouvernance complet de la sécurité de l'information traitée par l'État ; établit un SMSI conforme à ISO/IEC 27001 et avec les précisions requises par cette norme.
2-0	PSI-Perso	**Politique de gestion de données à caractère personnel**	Transpose des exigences de la règlementation en matière de protection des données à caractère personnel.
3-0	PSI-PSDC	**Politique de conservation**	Transpose des exigences de la loi du 2 juillet 2015 relative à la dématérialisation et à la conservation de documents.
4-0	PSI-Déontologie	**Code de déontologie**	Établit un code de déontologie de l'État en matière de sécurité de l'information.
5-0	PSI-Risques	**Gestion des risques**	Définit les objectifs et exigences pour la gestion des risques liés à la sécurité de l'information.
6-0	PSI-ORG	**Organisation de la sécurité**	Décrit les rôles et responsabilités ainsi que les exigences sur les processus de gestion de la sécurité de l'information. Clarifie le traitement des dérogations et des exceptions.
7-0	PSI-RH	**Sécurité liée aux ressources humaines**	Définit les objectifs et exigences liés aux ressources humaines.
8-0	PSI-Actifs	**Gestion des actifs**	Définit les objectifs et exigences pour la gestion des actifs, en particulier les informations et les systèmes d'information.
9-0	PSI-Accès	**Contrôle d'accès**	Définit les objectifs et exigences du contrôle d'accès, p.ex. l'utilité de l'authentification forte.

Les politiques générales par domaine (2/2)

Id.	Acronyme	Nom du domaine ou nom de la politique de sécurité	Commentaire
10-0	PSI-Crypto	**Cryptographie**	Définit les objectifs et exigences pour l'usage de la cryptographie.
11-0	PSI-Physique	**Sécurité physique et environnementale**	Définit les objectifs et exigences de sécurité physique et environnementale.
12-0	PSI-Exploit	**Sécurité de l'exploitation**	Définit les objectifs et exigences sécurité de l'exploitation des systèmes d'information.
13-0	PSI-Comm	**Sécurité des communications**	Définit les objectifs et exigences de la sécurité des réseaux de communications, p.ex. interne, réseau de l'État, messagerie électronique.
14-0	PSI-Systèmes	**Acquisition, développement et maintenance**	Définit les objectifs et exigences pour l'acquisition, le développement et la maintenance des systèmes d'information.
15-0	PSI-Fournisseurs	**Relation avec les fournisseurs**	Définit les objectifs et exigences pour la relation avec les fournisseurs.
16-0	PSI-Incidents	**Gestion des incidents liés à la sécurité de l'information**	Définit les objectifs et exigences assurant une gestion adéquate des incidents liés à la sécurité.
17-0	PSI-Continuité	**Gestion de la continuité de l'activité**	Définit les objectifs et exigences pour assurer la continuité de l'activité même en cas d'incidents importants.
18-0	PSI-Conformité	**Conformité**	Définit les objectifs et exigences pour assurer la conformité par rapport aux exigences légales, par rapport aux exigences contractuelles et par rapport à cette politique.
19-0	PSI-Class	**Politique de sécurité pour informations classifiées**	Définit le cadre de gestion et les objectifs liés à la gestion des informations classifiées, spécifie les exigences particulières pour les données classifiées LU Secret, LU confidentiel et LU restreint.

Le système de management de la sécurité de l'information

Définition de la PSI-SMSI

Système de management visant à établir, mettre en oeuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métier.

Note. Un SMSI se base sur l'appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisme pour traiter et gérer efficacement les risques.

Définition de la sécurité de l'information

« Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. »

Objectifs de la PSI-SMSI

- Repris de la norme ISO/IEC 27001, qui est applicable à toute entité, grande ou petite.
- Définir les exigences (inscrites dans cette norme) en matière de Système de Management de la Sécurité de l'Information.

Le futur SMSI de l'État

Exigences en matière de SMSI (selon ISO 27001)

Quand implémenter ? (1/3)

Étapes d'implémentation pour les entités de l'Etat

Phase de transition jusqu'à fin 2017

- Le CTIE s'est proposé de mettre en œuvre la PSI-LU d'ici fin 2016 dans le cadre d'un POC. Une analyse des risques sommaire pourra être entamée au sein de quelques entités volontaires. Après évaluation on pourra réviser les exigences et proposer un premier plan de mise en application début 2017.
- A partir de 2017: d'autres administrations disposant d'une propre infrastructure informatique d'une certaine envergure devront mettre en œuvre la PSI-LU.
- A partir de cette même année, une analyse des risques sommaire sera entamée auprès des autres entités, ceci avec l'assistance de l'ANSSI. Ceci permettra d'identifier les priorités au niveau de l'implémentation de la PSI-LU de sorte à pouvoir dresser un plan d'implémentation définitif pour 2018.

Le dirigeant de chaque entité maintient son droit de décider sur des exceptions par rapport à la PSI-LU, à condition que ces exceptions soient argumentées, ponctuelles et formellement documentées.

Quand implémenter ? (2/3)

Modèle d'organisation d'une implémentation

Phase préliminaire

- Décisions de base du dirigeant en fonction du niveau de maturité de l'entité, décision si SMSI dédié à l'administration ou SMSI au niveau du Ministère de tutelle.
- Attribution rôles DSI et DSSI.

Première phase d'implémentation

- Description contexte de l'entité et des objectifs spécifiques.
- Analyse des risques sommaire et documentation des actifs.
- Attribution d'autres rôles en matière de sécurité.

Quand implémenter ? (3/3)

Modèle d'organisation d'une implémentation

Deuxième phase d'implémentation

- Programme de sensibilisation, plan de communication.
- Appréciation des risques et acceptation risques résiduels.
- Revue de direction.

Phase de continuation de l'implémentation

- Revue documentations, appréciation et traitement des risques, plan d'action pour atteindre les objectifs de sécurité.
- Inventaire des écarts par rapport à la PSI-LU, audit interne.

Vous avez besoin d'informations ?

info@anssi.etat.lu

Tél. 247-88935

Merci pour votre attention.

Jerry Caye