ANSSI.lu

Agence nationale de la sécurité des systèmes d'information Luxembourg

La sécurité de l'information dans les entités étatiques

20 octobre 2017

Léon TREFF

Sujets de la présentation (1)

- **Sur le plan national**
  - Stratégie nationale en matière de cybersécurité
  - Politique de sécurité de l'information
    - Entités étatiques
    - Infrastructures critiques

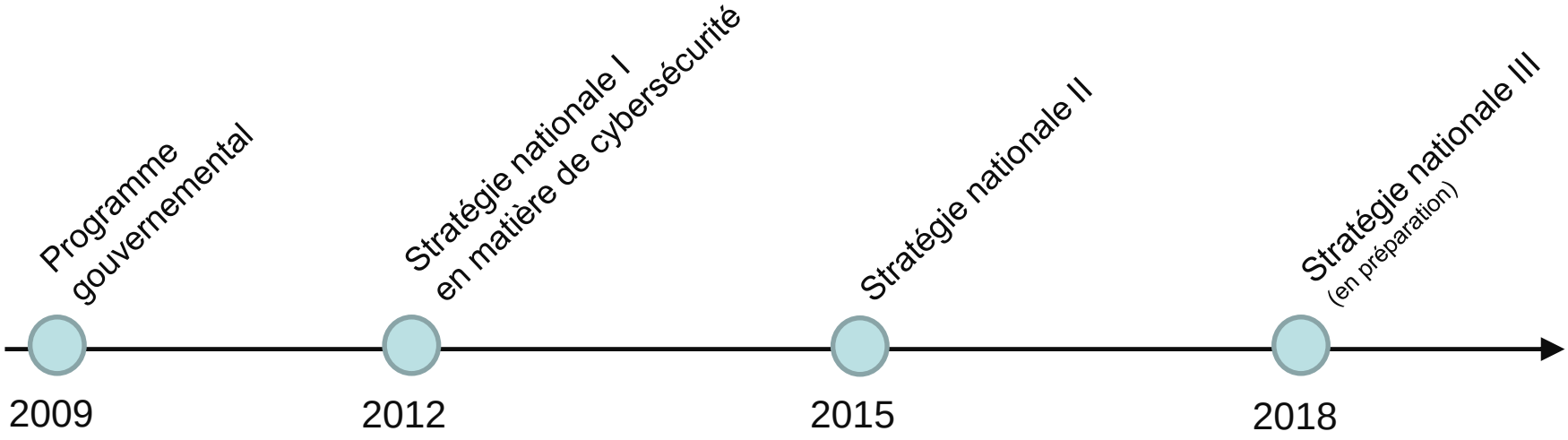
- **Sur le plan européen**
  - Directive « NIS »
    - Opérateurs de services essentiels (OSEs)
    - Fournisseurs de services numériques (FSNs)

Sujets de la présentation (2)

Sur le plan national

Stratégie nationale

Objectif: Protection adéquate des informations traitées dans les systèmes d'information



- Protection des infrastructures IT
- Prévention aux risques via CASES

5 axes:

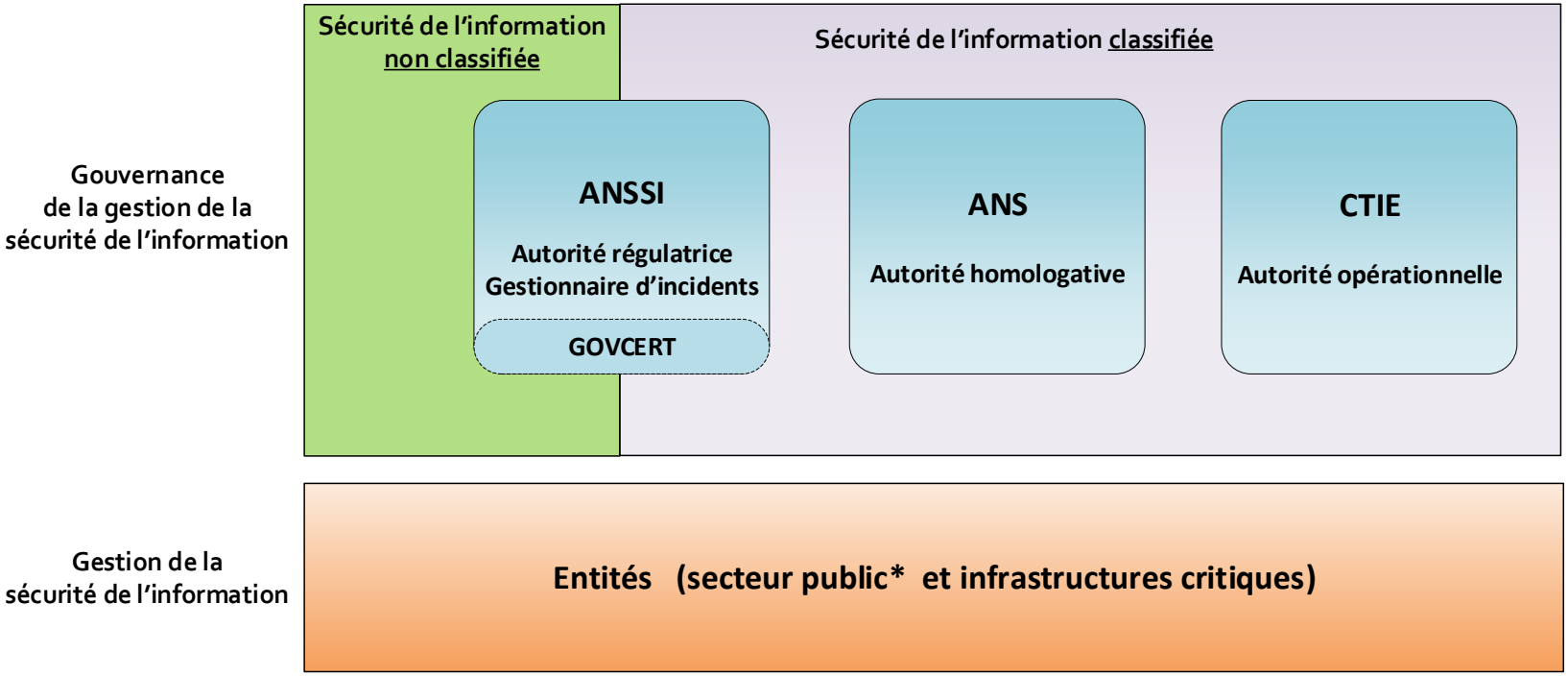
- Assurer protection opérationnelle des infrastructures IT
- Moderniser cadre légal
- Développer coopération
- Informer, éduquer, sensibiliser sur les risques encourus
- Mettre en place normes et standards

7 objectifs:

- Renforcer coopération nationale (e.a. création de l'ANSSI)
- Renforcer coopération internationale
- Augmenter résilience des infrastructures IT
- Combattre cybercriminalité
- Informer, éduquer, sensibiliser sur les risques encourus
- Mettre en place normes, standards, certificats, labels et référentiels d'exigences pour l'État et les IC
- Renforcer la coopération avec monde académique et de recherche

Gouvernance

Gouvernance de la gestion de la sécurité de l'information classifiée et non-classifiée



ANSSI : Autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés installés et exploités par l'Etat et les opérateurs d'infrastructures critiques pour leurs besoins propres.

* à l'exclusion des pouvoirs législatif et juridique, établissements publics et administrations communales

➢ Missions principales de l'ANSSI

- élaborer la Politique de Sécurité de l'Information de l'État luxembourgeois

  - définir les politiques et **lignes directrices** en matière de la sécurité de l'information classifiée et non classifiée et en **surveiller l'efficacité et la pertinence**

  - veiller à ce que les **mesures** concernant la sécurité des systèmes d'informations soient **mises en place** et que leur **application soit garantie**

→ assister les entités à mettre en œuvre la politique de sécurité de l'information

→ assister les entités à effectuer une analyse de risque

Politique de sécurité de l'information

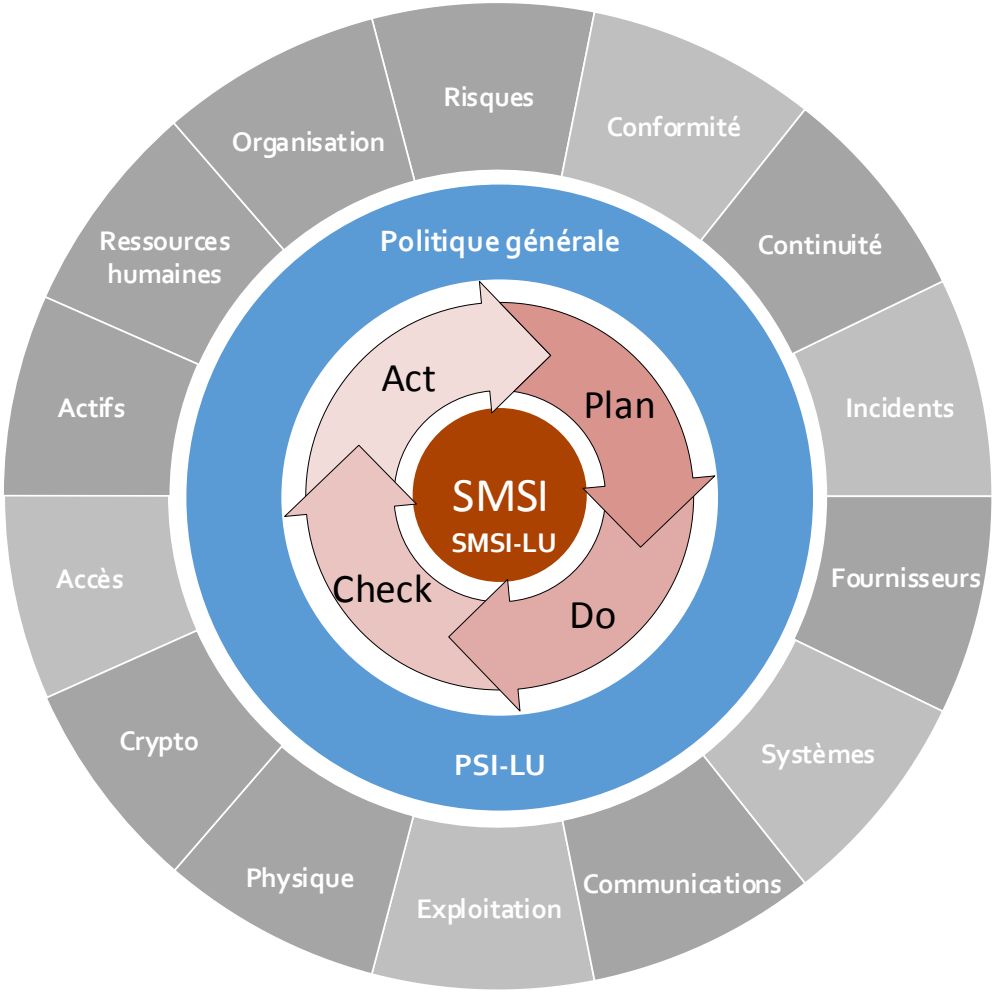
➢ La Politique de Sécurité de l'Information de l'État luxembourgeois (PSI)

- permet de mettre en œuvre la stratégie de cybersécurité
- constitue l'outil principal de la gouvernance de la sécurité des informations internes à l'État
- contribue au développement de la société numérique dans l'esprit de l'initiative « Digital Lëtzebuerg »

(Source: Digital Lëtzebuerg)

Gestion de la sécurité de l'information (1)

PSI-LU, PSI-SMSI et politiques par domaine



Pièces classifiées

Accès aux documents de la PSI

- **Publiés sur govSpace :**

  pour tous les utilisateurs avec compte IAM (du CTIE):
  https://govspace.msp.etat.lu/Pages/default.aspx

- **Sur demande auprès de l'ANSSI :**

  info@anssi.etat.lu

Exigences en matière de SMSI

Contexte	• Champ d'application • Besoins et attentes des parties prenantes • Références légales
Leadership	• Engagement par rapport aux objectifs de sécurité • Support du dirigeant • Rôles et responsabilités
Planification	• Analyses des risques • Actions liées aux risques • Objectifs de sécurité et plans d'action
Support	• Ressources et compétences • Sensibilisation, communication • Gestion de la documentation
Fonctionnement du SMSI	• Planification des mesures • Appréciation des risques • Traitement des risques
Évaluation des performances	• Surveillance • Audit interne • Revue de direction
Amélioration	• Non-conformité • Actions correctives • Amélioration continue

Gestion de la sécurité de l'information (2)

➢ Responsabilités du dirigeant de l'entité

- assumer la responsabilité globale de la sécurité de l'information
- intégrer la sécurité de l'information dans tous les processus et projets métier
- piloter et assurer la sécurité de l'information
  - » Stratégie et objectifs
  - » Gestion des risques
  - » Organisation
  - » Ressources
  - » Formation et sensibilisation
- évaluer les impacts
- apprécier les risques
- adopter un comportement exemplaire

Assistance à la mise en œuvre

➢ Approche graduelle (progressive)

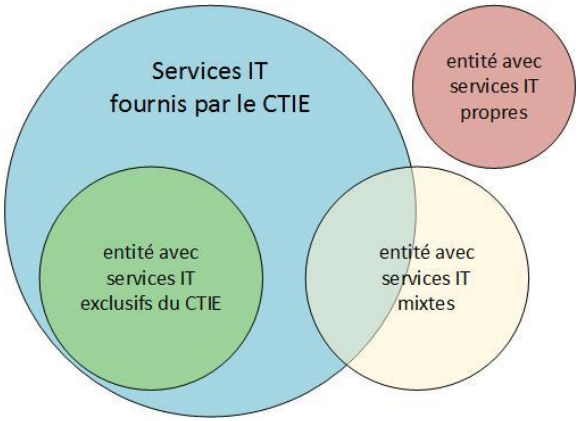
1. Charte de bonne conduite en matière de sécurité de l'information numérique

   (diffusion par lettre circulaire du Premier Ministre en date du 12.7.2017)

2. Mesures techniques à 3 niveaux,
   orientées principalement aux systèmes d'information
   (diffusion aux services IT prévue pour automne 2017)

3. Analyse de risque (qualitative)
   - » réalisée avec l'outil MONARC
   - » basée sur 3 profils type d'entité
   - » plateforme de travail mis à disposition par l'ANSSI
   - » assistance d'un consultant/expert de l'ANSSI

   (en cours de réalisation)



4. Mise en œuvre des mesures de sécurité prioritaires,
   suite aux analyses de risque

5. Implémentation SMSI et politique de sécurité auprès des entités critiques

Portail de la cybersécurité

www.cybersecurity.lu ou www.anssi.lu

Sujets de la présentation (3)

Sur le plan européen

'Directive NIS'

Directive (EU) 2016/1148 … concerning measures for a high common level of security of network and information systems across the Union

La 'Directive NIS' représente la première réglementation sur la cybersécurité au niveau européen

Applicable à partir du 10 mai 2018

Objectif : assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

I. Capacités (ressources) améliorées sur le plan national
II. Coopération accrue sur le plan européen
III. Obligation d'établissement d'une gestion des risques et de déclaration d'incidents pour les opérateurs de services essentiels (OSEs) et fournisseurs de services numériques (FSNs)

I. Capacités améliorées sur le plan national

Stratégie nationale définissant les objectifs stratégiques, une politique appropriée et des mesures régulatrices

- Objectifs stratégiques, priorités et référentiel de gouvernance
- Identification de mesures de disposition, réaction et récupération
- Méthodes de coopération entre les secteurs public et privé
- Sensibilisation, formation et éducation
- Plans de recherche et de développement
- Liste d'acteurs impliqués dans l'implémentation de la stratégie

Les États membres doivent désigner :

- **Autorités nationales compétentes** (une ou plusieurs)
  - superviser l'application de la Directive sur le plan national
- **Point de contact unique**
  - fonction de liaison pour assurer la coopération transfrontalière
- **Computer Security Incident Response Teams** (CSIRTs) participant dans le réseau des CSIRTs
  - superviser les incidents sur le plan national
  - fournir des avertissements précoces, alertes, annonces et la diffusion d'informations sur les risques et incidents à des acteurs importants
  - réagir aux incidents
  - fournir des analyses dynamiques de risques et d'incidents et prise de connaissance au cas par cas

II. Coopération accrue sur le plan européen

Groupe de coopération NIS

- Planification
- Contrôle
- Échange de bonnes pratiques
- Déclaration et communication
- ENISA apporte conseils et expertise

Réseau des CSIRTs nationaux

- Échange d'information sur les incidents
- Coordination transfrontalière de la réaction aux incidents
- Exercices
- ENISA assure le secrétariat

III. Obligation de gestion des risques et de déclaration d'incidents pour les OSEs et FSNs

A. Opérateurs de services essentiels (OSEs)

Entreprises privées ou entités publiques

1. L'entité fournit un **service** qui est essentiel au maintien d'**activités sociétales et/ou économiques critiques** ;
2. la disponibilité de ce service **dépend** de réseaux et de systèmes d'information ; et
3. un incident de sécurité aura un **effet d'interruption significatif** sur la disponibilité de ce service essentiel.

'Directive NIS'

Secteurs concernés :

- **Énergie**: électricité, pétrole et gaz
- **Transport**: air, chemin de fer, eau et route
- **Banques** : institutions de crédit
- **Infrastructures du marché financier** : plateformes de marché, contreparties centrales
- **Santé** : prestataires de soins de santé
- **Eau** : approvisionnement et distribution d'eau potable
- **Infrastructure numérique** : points d'échange numériques, fournisseurs de services pour le système de noms de domaines, répertoires de noms de domaine principaux (top level domain name registries)

Les OSEs doivent :

- **établir des mesures de sécurité appropriées**
  - pour gérer les risques
  - pour assurer un niveau de sécurité approprié pour chaque risque
  - pour anticiper et minimiser l'impact d'incidents et assurer la continuité des services

- **notifier les incidents ayant un impact significatif sur la continuité des services essentiels à l'autorité nationale compétente**
  - sans délai inadmissible
  - fournir les informations nécessaires pour déterminer tout impact transfrontalier éventuel

B. Fournisseurs de services numériques (FSNs)
(Digital Service Providers) (DSPs)

Applicable aux activités numériques importantes (*)

FSNs dans le périmètre NIS

- Plateformes de marché en ligne (Online marketplaces)
- Services informatiques en nuage (Cloud computing services)
- Moteurs de recherche (Search engines)

Approche régulatrice "light-touch"

- Supervision "light-touch" et réactive ex post
- minimise la charge de conformité
- assure le bon fonctionnement du marché numérique unique

(*) n'est pas applicable aux micro- et petites enterprises telles que définies dans la Recommandation de la Commission 2003/361/EC (1).

Les FSNs doivent :

- **prendre des mesures de sécurité appropriées pour**
  - éviter les risques
  - assurer la sécurité des réseaux et systèmes d'information
  - traiter les incidents

  Note : Les FSNs sont libres de prendre les mesures qu'ils considèrent appropriées pour gérer les risques auxquels leurs réseaux et systèmes d'information sont exposés.

- **notifier les incidents substantiels à l'autorité nationale compétente**

Situation actuelle de l'implémentation de la Directive

- Les services essentiels doivent d'abord être identifiés,
  des critères et seuils doivent être définis (moyennant un règlement grand-ducal),
  ensuite les OSEs doivent être désignés (par arrêté grand-ducal)

- Les exigences de sécurité pour les OSEs ne sont applicables qu'aux services numériques qui sont critiques pour la fourniture des services essentiels

- Des exigences de sécurité de base seront basées sur des standards internationaux (p. ex. ISO/IEC 2700x) ;
  la contribution des OSEs est fortement appréciée

- Des exigences de sécurité sectorielles spécifiques peuvent être développées avec/par les secteurs

- Le dépôt d'un projet de loi à la Chambre des Députés est prévu pour Q1 2018

Fin de la présentation

Pour nous contacter:

email: info@anssi.etat.lu

ou

leon.treff@anssi.etat.lu
Tél. 247-88945

Merci de votre attention