La gouvernance informée: Le rôle du gouvernement dans la gestion des risques collaborative

.

François Thill, Director cybersecurity,
Ministère de l'Économie

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Agenda

- Introduction
- La troisième stratégie cyber
- Vers l'économie numérique
- Les bases de la gouvernance informée
- Ce qui se passe actuellement

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Leitmotiv

- La cybersécurité crée la confiance entre les citoyens et les entreprises. Cependant, sa mise en œuvre est **souvent discriminatoire du point de vue des coûts et de la complexité**.
- La cybersécurité représente une opportunité économique. **Nous croyons fermement en la responsabilisation de toutes les parties prenantes, dans le cadre de la démocratisation de la sécurité de l'information.**
- **La cybersécurité est une tâche collaborative** associant gouvernements, entreprises et particuliers.
- La cybersécurité concerne tout individu. Pour un pays qui construit ses atouts économiques sur les TIC, **la cybersécurité est un atout essentiel pour son attractivité économique.**.

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Inspirations pour le Leitmotiv

- **OCDE document 2002 -** Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: *vers une culture de la sécurité*
- **OCDE document: 2015 -** Recommandations de l'OCDE La gestion du risque de sécurité numérique pour la prospérité économique et sociale

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Cybersécurité - objectifs

- **Confidentialité** - donner accès uniquement aux utilisateurs autorisés (cryptologie, gestion des accès)
- **Intégrité** - empêcher les modifications non autorisées (hachage,…)
- **Disponibilité** - prévenir la destruction; planifier des ressources suffisantes

La cybersécurité crée la confiance - la confiance est essentielle au commerce et au développement des services d'administration en ligne.

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Gouvernance du côté gouvernemental

- **Cybersecurity Board:** coordination stratégique sous la responsabilité du Premier ministre
- **Groupe de coordination interministériel (CIC):** coordination tactique sous la responsabilité de HCPN
- **CERC** Cellule d'Evaluation du Risque Cyber: détection de crises
- **PLAN Cyber**

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Régulateurs

- **CNPD** – autorité de contrôle pour la protection des données
- **CSSF** – autorité de contrôle pour le secteur bancaire et NIS
- **ILR** – régulateur télécom et NIS
- **HCPN** – Haut Commissariat à la Protection Nationale
- **ILNAS** – régulateur pour la dématérialisation et la conservation

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Cybersécurité - approche

- **Comportement** - les **utilisateurs** doivent être conscients des menaces
- **Organisation** - gestion des risques, politiques, procédures, normes
- **Technique** - outils et services de prévention, de détection et mitigation

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Sensibilisation (comportement)

- **Bee-Secure** - depuis 2008 (Economie, Famille, Education)
  - Chaque enfant à l'âge de 10 ans
  - Chaque enfant à l'âge de 13 ans
  - Campagnes nationales à grande échelle
- **CASES** – depuis 2002 (Economie - créé après “I love you”)
  - **Chaque nouveau fonctionnaire**
  - **Campagnes** dans la plupart des ministères et des administrations

Introduction

Procédures, politiques, outils (organisation)

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- **CASES**
  - Méthodologie collaborative de gestion des risques MONARC
    - Réduction de l'effort individuel de 80%
  - Publication des politiques et procédures: www.cases.lu
- **ANSSI** - depuis 2015 (HCPN)
  - Publication d'une politique
  - Déploiement de la gestion des risques avec l'aide de la MONARC dans les ministères et les administrations

Introduction

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

CERTs - technique

- CIRCL - depuis 2010 (securitymadein.lu)
  - Réponse sur incidents pour le secteur privé et les communes
  - Crée de nombreux outils open source et donne accès aux informations relatives à la sécurité
    - MISP (outil standard de collaboration et d'échange de menaces)
    - AIL (analysis of information leak)
    - BGP-ranking
    - D4
    - 10 autres
- GovCERT - depuis 2011 (HCPN)
  - Réponse sur incidents pour le gouvernement et les opérateurs d'infrastructures critiques, prévention, détection et mitigation
- **Restena** CSIRT et **Healthnet** CSIRT

Introduction

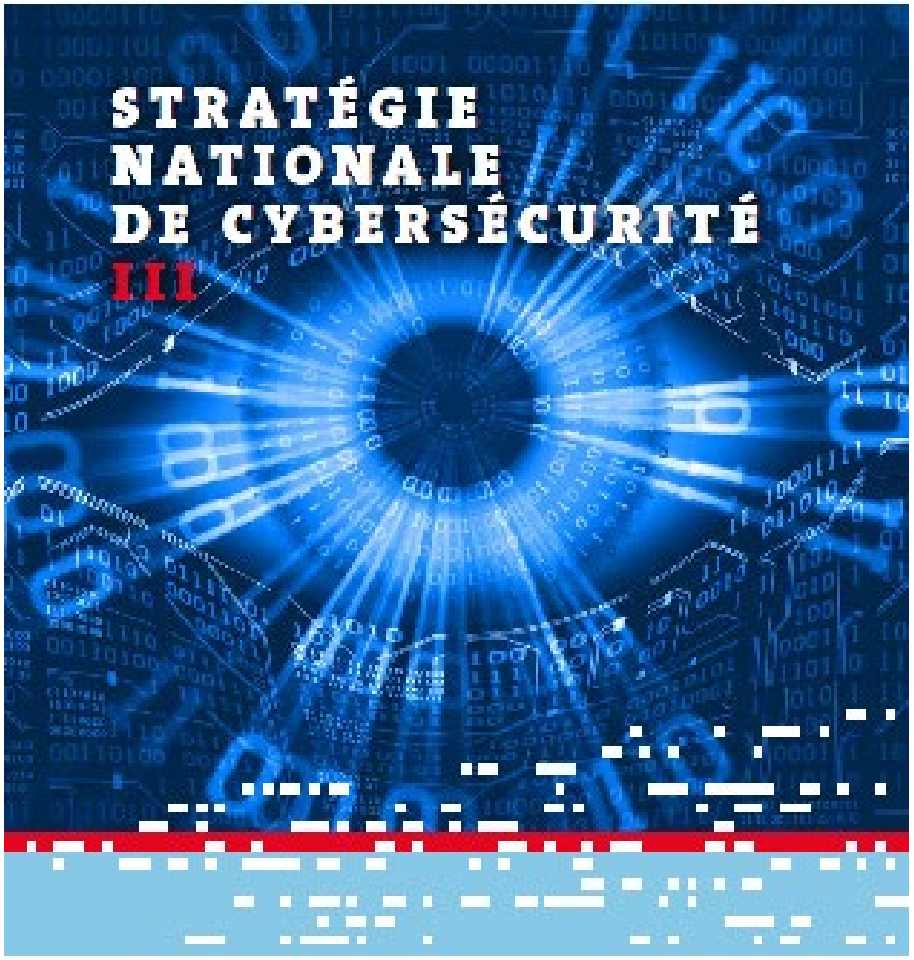
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Cybersecurity Competence Center (C3) depuis 2017

- Objectif principal: PPP pour créer des services supportant une économie numérique
- **Observatoire**
  - Coopération avec la cyberassurance
- **Formations**
  - “Room42” : C-level training pour gérer des crises cyber
    - Avec un nouveau scénario RGPD
- **Testing**
  - Tests et due diligence pour les start-ups

La troisième stratégie cyber

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



La troisième stratégie cyber

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Structure : trois lignes directrices

- Renforcer **la confiance publique** dans l'environnement numérique
- Protection des **infrastructures** numériques
- Promotion de la place **économique**

avec 22 objectifs et 61 mesures

La troisième stratégie cyber

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Renforcer la confiance publique - objectifs

- Partage des connaissances entre toutes les parties prenantes
- **Diffuser des informations sur les risques**
- Sensibilisation de toutes les parties concernées
- Divulgation responsable
- La lutte contre la cybercriminalité

La troisième stratégie cyber

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Protection des infrastructures numériques - objectifs

- Recensement des infrastructures essentielles et critiques
- Politiques de sécurité
- **Gestion de crise – équipes d'intervention**
- Standardisation
- Renforcer la coopération internationale
- Cyberdéfense
- Renforcer la résilience de l'infrastructure numérique de l'État

La troisième stratégie cyber

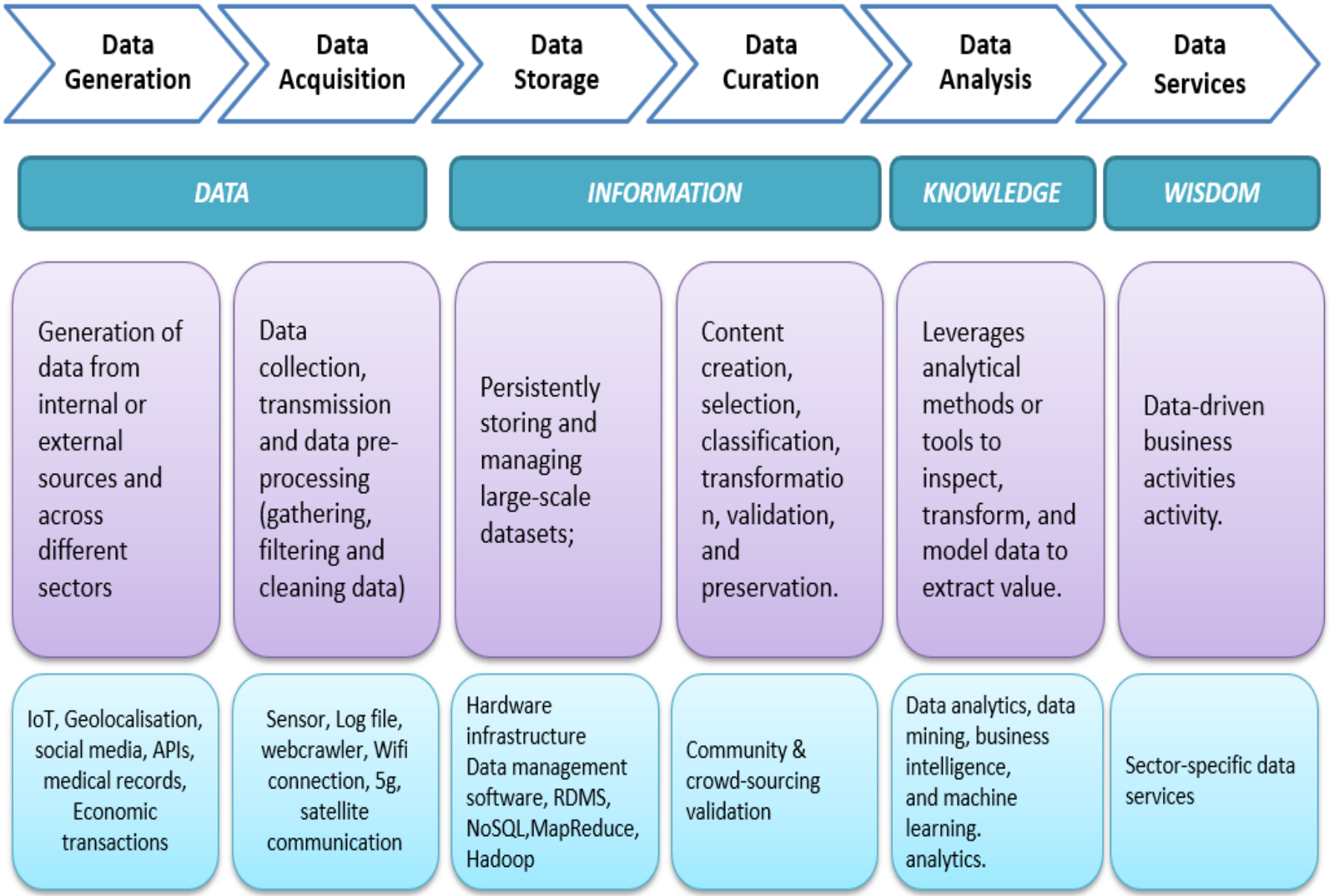
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Promotion de la place économique

- Création de nouveaux produits et services
- Mutualisation des infrastructures de sécurité
- Référentiels d'exigences et maître d'oeuvre
- Création du centre de compétences en cybersécurité (C3)
- **Gestion des risques et gouvernance informée**
- Formation et aide à la formation
- **Collaboration entre responsables de la sécurité de l'information**
- **Collaboration entre experts en matière de réponse aux incidents**
- Priorité à la recherche : les start-ups
- Le désassemblage du code et identification des vulnérabilités

Vers l'économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** doit promouvoir la réutilisation des données (HPC^3):

- **Gestion du consentement**, conformité au RGPD
- Micro-compensations
- TTP, **pseudonymisation** (**A-35**), techniques **d'anonymisation**
- Concepts de filtrage de données (gestion des attributs - minimisation des données)
- **Empêcher la réidentification** des personnes concernées
- Réduction des détails, granularité (ajustement des courbes, lissage)
- Flouetage et abstraction pour réduire la criticité
- Data broker
- Transfert de données à l'intérieur et à l'extérieur de l'UE
- Authentification, gestion des droits, cryptage, décentralisation

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** a besoin d'infrastructures telles que:

- Réseaux d'alerte précoce (**A-39**)
- DDOS mitigation mutualisée, boucle locale (**A-43, A-44**)
- Des concepts comme l'ambassade électronique (**A-36**)
- Le HPC

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** nécessite des normes harmonisées en matière de sécurité et une guidance claire (DSM):

- Exigences minimales de sécurité, en fournissant des scénarios et des politiques (**A-34**: secteur des assurances)
- Fournir des contrats types de sous-traitance (**A-45**)
- Créer des normes certifiables (**A-41**)

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** a besoin de catalyseurs puissants:

- Favoriser la création de PPP pour relever les défis nationaux et internationaux (**A-34**)
- Formation d'équipes multidisciplinaires (**A-48**)
- Cyber simulateur et essais (**A-49**)
- Le High Performance Computing Competence Center **HPC^3**

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** nécessite INTEL:

- Taxonomie de gestion des risques
- Fournir une situational awareness (**A-33**, **A-37**, **A-38**, **A-42**)
- Principaux scénarios de risques (**A-51** Risk Information Sharing Platform)
- Fournir des métriques pour la gestion des risques (**A-54**)
- Gouvernance par la gestion des risques (**A-53**)

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** a besoin d'experts:

- Offrir des formations appropriées (**A-46**, **A-47**, **A-52**)
- Fournir des programmes d'aide à la formation (**A-56**)
- Master auprès de uni.lu pour la cybersécurité (**A-55**)

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Dans une **économie numérique**, les experts doivent collaborer:

- Promouvoir la création de RSSI au sein des entreprises (**A-57**)
- Améliorer les réseaux de collaboration pour les **RSSI** et les **DPO**

Vers une économie numérique

Dans une **économie numérique**, les CERT doivent collaborer:

- Vers de plus grandes capacités de gestion des incidents privés (**A-58**, **A-59**) avec l'aide du secteur des assurances

Vers une économie numérique

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une **économie numérique** a besoin de services spécialisés:

- Favoriser la création de start-ups en cybersécurité (**A-40**)
- Favoriser la sécurité dans les incubateurs (**A-60**)
- Fournir des installations spécifiques de test de start-ups (**A-50**)

Vers une économie numérique

Une **économie numérique** doit traiter les vulnérabilités:

- Promouvoir la divulgation responsable (**A-61**)
- Créer un réseau de scans de vulnérabilités

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Photo: Monceau

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Les **interdépendances** entre les systèmes sont de plus en plus complexes, la cyber-sécurité **n'est plus un défi individuel**, il y a trop en jeu.
- Les décisions en matière de gestion des risques doivent être **fiables**, **comparables** et **reproductibles**.
- **Les décisions en matière de gestion des risques** doivent être prises sur base d'informations aussi **factuelles** que possible.

- La **collaboration est un MUST, des taxonomies communes sont nécessaires**
- Une **guidance coordonnée** est nécessaire.

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Gestion des risques - **choix de gouvernance**:

- Actifs primaires (portée)?
- Scénarios de risque (granularité)?
- Qualification des impacts ?
- Qualification des menaces?
- Qualification des vulnérabilités?
- Décisions d'atténuation des risques?
- Efficacité des mesures mises en place?
- Matrice d'acceptation des risques?

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Primary assets (scope)
- Risk scenarios (granularity)
- Qualification of impacts
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions
- Effectiveness of risk treatment measures
- Risk acceptance matrix

Comment choisir des scénarios de risque pertinents?

- Les incidents les plus fréquents dans une PME peuvent être décrits par **42 scénarios** (diagnostic CASES).
- Les **CERT** et les **SOC** connaissent souvent les scénarios qui ont conduit à des incidents.
- Les **régulateurs** ont déjà ou auront cette information (notification de fuites de données et d'incidents)
- **ENISA** et autres paysages de la menace
- Les **entreprises de sécurité spécialisées** ont beaucoup d'expérience

PARTAGEZ ces informations précieuses pour le bien de tous

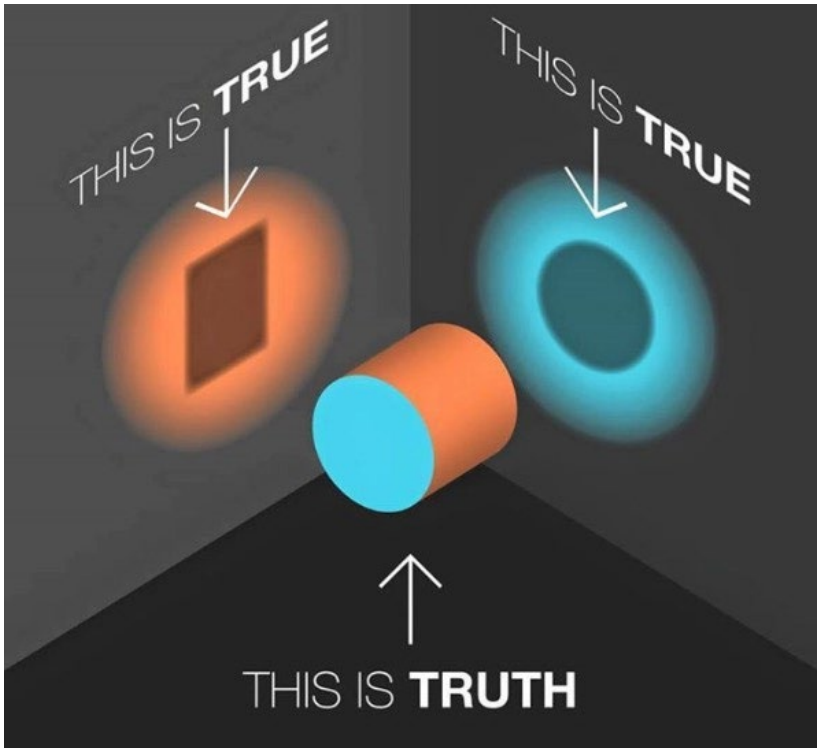
Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Primary assets (scope)
- Risk scenarios (granularity)
- **Qualification of impacts**
- Qualification of threats
- Qualification of vulnerabilities
- Risk treatment decisions
- Effectiveness of risk treatment measures
- Risk acceptance matrix

Comment choisir la qualification d'impact(s)?

- Pour vous-même
- Pour les personnes concernées
- Pour vos clients

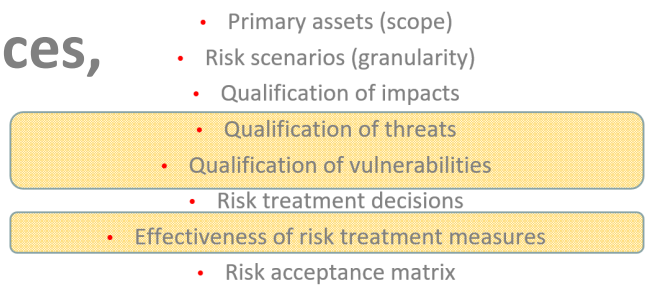


Maggie Hos-McGrane

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Comment **qualifier les menaces, vulnérabilités et l'efficacité des mesures**?



- Projecs comme MISP*, AIL**, D4***, BGPRanking**** peuvent fournir des indications
- **ENISA** et autres paysages de la menace
- Les **SOC** et les **entreprises de sécurité spécialisées** ont beaucoup d'expérience

*: MISP - https://www.circl.lu/services/misp-malware-information-sharing-platform/
** AIL: https://www.circl.lu/services/ail-training-materials/
*** D4: https://d4-project.org/
****: BGPRanking: https://www.circl.lu/projects/bgpranking/

Les bases d'une gouvernance informée

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Gouvernance informée grâce à la collaboration

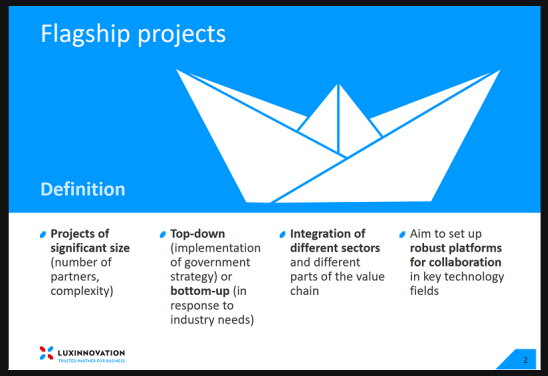
- Actifs primaires (portée)?
- Scénarios de risque (granularité)
- Qualification des impacts ?
- Qualification des menaces
- Qualification des vulnérabilités
- Décisions d'atténuation des risques?
- Efficacité des mesures mises en place
- Matrice d'acceptation des risques?

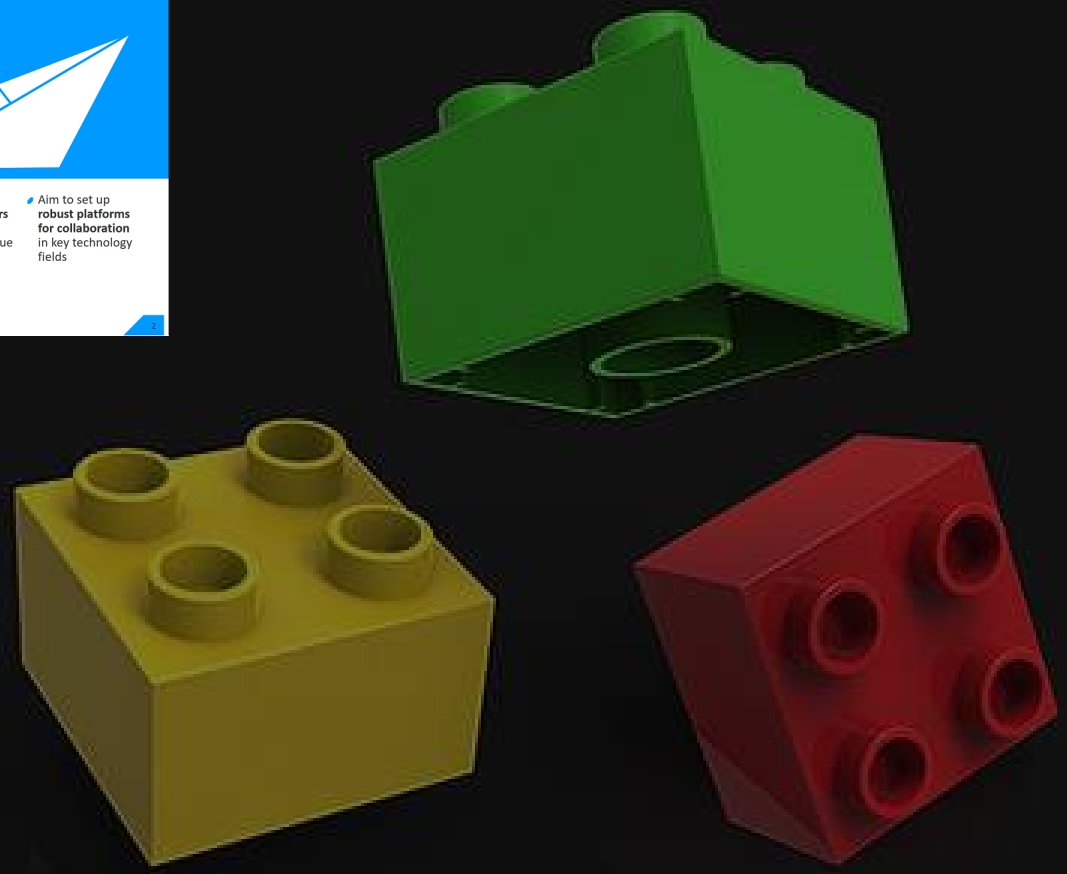
Collection de scénarios d'incidents fréquents

Informations fournies par les CERT & SOC

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG





Jürgen Lousberg

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Les données brutes doivent être distillées dans une "situational awareness" (**A-42**)
  - Création d'une taxonomie commune
  - Creation de **dashboards**
- La SA et les incidents doivent être distillés en scénarios & métriques (**A-54**)
  - Sélection de scénarios communs
    - ANSSI & GovCERT au sein du gouvernement
    - **Luxinnovation Flagship projet dans le secteur privé**
  - Qualification de
    - Menaces
    - Vulnérabilités
    - Efficacité des traitements

Ce qui se passe actuellement

- Création et publication de **normes de sécurité de base**
  - Certification dans le cadre du cyber-act (**A-41**)
    - Niveau Basique
  - Création de lignes directrices (**A-52**)
  - Établissement de la confiance dans une économie numérique
  - Devenir un **standard pour le secteur des assurances**, un important régulateur informel (**A-34**)

Ce qui se passe actuellement

- Recontextualisation dans les secteurs
  - Création d'ISAC sectoriels (Centre de partage et d'analyse d'informations) (**A-59**)
  - **Enrichissement des scénarios** par ISAC sectoriel
  - **Enrichissement des normes de sécurité de base** par ISAC sectoriel
  - **Certification** dans le cadre du **cyber**-act (**A-41**)
    - Niveau Avancé

Vers une plate-forme de partage d'informations sur les risques

(Monarc Object Sharing Platform)

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une gouvernance informée basée sur la collaboration

- Actifs primaires (portée)
- Scénarios de risque (granularité)
- Qualification des impacts?
- Qualification des menaces
- Qualification des vulnérabilités
- Décisions d'atténuation des risques?
- Efficacité des mesures mises en place
- Matrice d'acceptation des risques?

Collecte des incidents fréquents fournis par SA & ISAC et RISP

Informations fournies par Situational Awareness, ISAC et RISP

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Meilleure harmonisation du cadre réglementaire en matière de cybersécurité
  - **Implication des régulateurs dans une phase précoce, donnant des conseils et des conseils**
  - **Collaboration internationale des régulateurs**
    - RGPD: CNPD – EDPB
    - NIS: ILR – groupe de collaboration européen
  - Vers une collaboration transversale des régulateurs?

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Une gouvernance informée basée sur la collaboration

- Actifs primaires (portée)
- Scénarios de risque (granularité)
- Qualification des impacts
- Qualification des menaces
- Qualification des vulnérabilités
- Décisions d'atténuation des risques?
- Efficacité des mesures mises en place
- Matrice d'acceptation des risques

Régulateur

Par la communauté

Ce qui se passe actuellement

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Nous avons la mission de faire de notre mieux

« …

Les référentiels d'exigences des différents régulateurs dans le domaine des données numériques et de la cybersécurité seront harmonisés. **Un système de régulation qui évite les doubles emplois constitue un avantage compétitif et permettra au Luxembourg de gagner en efficacité et en attractivité, dans le respect de la protection des données**.

… »*

*: https://gouvernement.lu/de/publications/accord-coalition/2018-2023.html

L’approche vit de l’abstraction et de la recontextualisation et non de la COMPLEXITÉ

Il est hautement collaboratif et évolutif

et d'une importance capitale pour notre économie

LUXEMBOURG

LET'S MAKE IT HAPPEN

LET'S MAKE IT HAPPEN