LUXEMBOURG

LET'S MAKE IT HAPPEN

CYBERSECURITY IN LUXEMBOURG

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

Leitmotiv

- Cyber security concerns any individual. For a country building its economic strengths on ICT, **cyber security is an essential asset to its economic attractiveness**.
- Cyber security creates trust among citizens and businesses. However its implementation **is often discriminatory from the point of view of costs and complexity**.
- Cyber security represents an economic opportunity. **We strongly believe in the empowerment of all the stakeholders, as part of the democratisation of information security.** Our approach is customer oriented, collaborative and coordinated at national level.
- **Cybersecurity is a collaborative task**, involving governments, companies and individuals.

Leitmotiv – inspired by

- **OCDE document 2002 -** OECD Guidelines for the Security of Information Systems and Networks: *Towards a Culture of Security*
- *Cybersecurity as a service from the Ministry of the Economy*
- **OCDE document: 2015 -** Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

Cybersecurity - target

- **Confidentiality** – give access to authorized users only (cryptology, access management)
- **Integrity** – prevent unauthorized modification (hash, …)
- **availability** – prevent disruption, implement resilience

Cybersecurity creates trust – trust is essential for business and development of e-government services

Cybersecurity - approach

- **Behavior** – the **users** must be aware about threats
- **Organisation** – risk management, policies, procedures, standards
- **Technology** – prevention, detection and mitigation tools and services

Governance

- **Cybersecurity Board: strategic coordination under the responsibility of the Prime Minister**
- **Inter-ministerial Coordination Group (CIC): tactical coordination under the responsibility of HCPN**
- **CERC (cellule d'évaluation du risqué cyber): detection of crisis**
- **Cyber Crisis Plan**
  - As an example: National DDoS mitigation platform controlled by HCPN

WHAT WE DO

Regulators

- **CNPD** – data protection authority
- **ILR** – telecom regulator and NIS (network and information security directive)
- **CSSF** – banking authority (also NIS)
- **HCPN** – critical infrastructure regulator
- **ILNAS** – regulator for dematerialization and conservation

➔**harmonization** of the regulator's requirements would create a substantial factor of attractiveness; **informed governance is a priority**

Awareness - behavior

- Bee-Secure – since 2008 (Economy ,Family, Education)
  - Every kid at the age of 10
  - Every kid at the age of 13
  - Large scale national campaigns
- CASES – since 2002 (Economy - created after “I love you” virus)
  - Every new civil servant
  - Campaigns in most of the ministries and administrations
  - Rewarded twice as best practice from ENISA

Organization – procedures, policies

- **CASES** – since 2002 (Economy - created after “I love you” virus)
  - Collaborative Risk management methodology MONARC: link
    - Reduction of the individual effort by 80%
  - Publication of Policies and procedures: www.cases.lu
- **ANSSI** – since 2015 (HCPN)
  - Publication of a governmental cyber security policy
  - Deployment of risk analysis within the government with the help of MONARC

Technical – Computer Emergency Response Teams

- **CIRCL** – since 2010 (one brand of securitymadein.lu)
  - Incident response for private sector and communes
  - Creates a lot of open source tools an gives access to security relevant information
    - MISP (standard tool for collaboration and exchange of threat): link
    - AIL (analysis of information leak): link
    - BGP-ranking: link et plate-forme
    - 10 more (list of services)
- **GovCERT** – since 2011 (HCPN)
  - Incident response for government and operators of critical infrastructures
- 10 CERTs federated under **CERT.lu**
  - 4 public (GovCERT, CIRCL, Restena, Healthnet)
  - 7 private
- Creation of **situational awareness** by Luxembourg CERTs

Cybersecurity Competence Center (C3) - 2017

- **Main objective: PPP for the establishment o services we need for the deployment of the data driven economy:** link
- **Observatory**
  - From situational awareness towards organizational security
    - Objective metrics for risk management (taxonomies, threat probabilities, ease of exploitation of vulnerabilities, efficiency of risk treatment)
    - Guidance for risk management (selection of scenarios)
    - Early warning
  - Cooperation with cyber-insurance, informal regulator for unregulated SME
  - RISP – Risk Information Sharing Platform
- **Training**
  - Room42 – C-level training for cyber crisis, additional GDPR scenario added recently
- **Testing**
  - Testing and due diligence for start-ups

Fostering collaboration within the ecosystem

- Luxembourg has a **large and competent cyber security ecosystem**
- Organisation of the **monthly cyber security breakfast** by securitymadein.lu **for private sector**
- Organisation of **recurrent cyber security breakfasts within government** organized by GovCERT
- CERT.lu initiative with their recurrent meetings
- List of the members of the ecosystem: https://securitymadein.lu/ecosystem/
- Creation of a cyber security ecosystem cartography by Luxinnovation and securitymadein.lu

Promotion of the ecosystem benefits

- **Trade missions:**
  - **outbound** missions to promote the competences of our ecosystem members
  - **Inbound** to attract needed parts for the development of the Luxembourg economy

LOOKING FOR

International cooperation – informed governance

- **Risk management must become comparable and reproducible**
- **Publish metrics necessary for risk management (risk management is a collaborative task):**
  - **Define a common risk taxonomy**
  - **Publish scenarios that are important**
    - Threat (probability)
    - Vulnerability
    - Impact
  - Publish qualitative metrics for
    - Threat
    - Vulnerabilities
    - impacts
  - Build interdependence models (possible due to common taxonomy and metrics)
- **Harmonize** requirements of different regulators

LOOKING FOR

International cooperation – incident response

- Create **international Intervention teams** (CERT)
- Foster the use of **collaborative tools** like MISP, AIL, RISP, D4, MONARC
- Foster **information sharing** in cyber security

LOOKING FOR

International recognition

- Create **certifiable standards** (Cyber Package and GDPR)
  - Pseudonymisation
  - Anonymization
  - Data broker

LUXEMBOURG

LET'S MAKE IT HAPPEN

LET'S MAKE IT HAPPEN