LËTZ PREPARE ! STRATÉGIE NATIONALE DE RÉSILIENCE

PILIER 6

La cyberrésilience

Nous dépendons de plus en plus des technologies numériques dans notre vie quotidienne, notre économie et nos institutions. Pour garantir la stabilité du pays et la confiance des citoyens, nous devons être capables non seulement de prévenir les cyberattaques mais aussi d'y résister, de nous en remettre et de nous adapter. Face à des menaces toujours plus sophistiquées, orchestrées par des acteurs étatiques et non-étatiques, la cyberrésilience repose sur une approche systémique et coordonnée : une gouvernance, une culture de gestion de crise et une communication efficaces ainsi que l'accès à des moyens techniques sont essentiels pour protéger et défendre nos réseaux et nos systèmes d'information.

Objectif : Renforcer les capacités de cyberrésilience du Luxembourg.

Les actions clés

PROTÉGEONS
Préparer l'avenir ensemble

Pour atteindre cet objectif, plusieurs actions sont définies, dont :

Pour renforcer la gouvernance nationale et la coordination stratégique :

- Nous révisons la stratégie nationale de cybersécurité afin de renforcer la confiance publique dans le monde numérique, protéger les droits humains en ligne, consolider la sécurité et la résilience des infrastructures numériques ainsi que de contribuer à développer une économie numérique fiable, durable et sécurisée.
- Nous continuons à renforcer la gouvernance et la coordination de l'écosystème national de cybersécurité afin d'optimiser la structure et l'harmonisation des efforts de cybersécurité à l'échelle nationale en impliquant les institutions et pouvoirs publics en charge de la cybersécurité et de la cyberdéfense, les entités critiques, les entreprises et les citoyens.

Pour renforcer les capacités opérationnelles :

- Nous protégeons les systèmes d'information critiques en améliorant les capacités opérationnelles, en mettant en place des capacités avancées de détection, en élaborant une connaissance partagée de la situation, en diffusant des alertes précoces et en partageant systématiquement des informations exploitables sur les menaces, les attaques et les tentatives d'intrusion, ainsi qu'en coopérant avec les acteurs nationaux concernés afin de renforcer le niveau de préparation à la gestion des incidents majeurs et des crises cybernétiques.
- Nous renforçons la coopération civilo-militaire à travers des mécanismes intégrés de gestion de crise, de partage d'informations, d'élaboration de normes interopérables, d'évaluation conjointe des risques et d'organisation d'exercices conjoints.
- Nous promouvons l'innovation dans le domaine de la cybersécurité et accélérons le déploiement d'outils luxembourgeois ou européens par des programmes de financement ou d'aides dans les domaines de la digitalisation, de la cybersécurité, du *quantum computing* et de l'intelligence artificielle.

Pour développer l'expertise et la sensibilisation :

- Nous continuons à développer l'expertise nationale en matière de cyberrésilience en coopérant avec les institutions de recherche publiques, en maintenant un haut niveau d'expertise et une maîtrise autonome des compétences, en développant l'expertise dans les technologies émergentes et d'outils autonomes pour les petites et moyennes entreprises ainsi qu'en adressant la pénurie de compétences dans le secteur de la cybersécurité.
- Nous promouvons l'éducation, la formation et la sensibilisation en matière de sécurité des systèmes d'information à travers la création de programmes spécifiques dans les cursus scolaires et des campagnes d'information et de sensibilisation.
- Nous accompagnons les entités régulées, en particulier les petites et moyennes entreprises, par le biais du développement de recommandations et d'outils.