N°4332
Entrée le 26.06.2026
Chambre des Députés
Déclarée recevable
Président de la Chambre des Députés
(s.) Claude Wiseler
Luxembourg, le 26.06.2026
Chambre des Députés

piraten.lu

PIRATEN

Claude WISELER
President vun der
Chamber vun den Deputéierten
19, um Krautmaart
L-1728 Lëtzebuerg

Lëtzebuerg, den 26/06/2026

**Här President,**

**Sou wéi den Artikel 80 vun eisem Chambersreglement et virgesäit, bieden ech lech, dës parlamentaresch Fro un de Premierminister & de Minister fir Wirtschaft weiderzeleeden.**

La loi du 28 mai 2019 portant transposition de la directive NIS1 a confié à l'Institut Luxembourgeois de Régulation (ILR) la mission de superviser la notification des incidents de sécurité affectant les opérateurs de services essentiels et les fournisseurs de services numériques. Bien que cette loi ait depuis été abrogée par la loi du 5 mai 2026 transposant la directive NIS2, il importe de dresser un bilan opérationnel de son application pour l'année 2025, dernière année pleine sous le régime NIS1.

An deem Zesummenhang wéilt ech de Ministeren dës Froe stellen:

1. Combien de notifications d'incidents de sécurité ont été reçues par l'ILR au titre de la loi du 28 mai 2019 sur cette période ? Le Ministre peut-il fournir une ventilation par secteur d'activité (énergie, transports, santé, eau, infrastructures numériques, services financiers, etc.) ?

2. Parmi ces notifications, combien ont été classifiées comme incidents « significatifs » au sens de la loi ? Quels critères de seuil l'ILR applique-t-elle en pratique pour déterminer le caractère significatif d'un incident ?

3. Quel est le délai moyen constaté entre la survenance d'un incident et sa notification à l'ILR par l'opérateur de services essentiels ou le fournisseur de services numériques ?

4. Dans combien de cas l'ILR a-t-elle jugé une notification incomplète ou tardive et quelles suites ont été données (demande de complément, avertissement, sanction) ?

5. Dans combien de cas l'ILR a-t-elle constaté qu'un incident aurait dû être notifié mais ne l'a pas été ? Quels mécanismes de détection des sous-notifications l'ILR a-t-elle mis en place ?

6. Combien de notifications ont donné lieu à une transmission au CSIRT national (CIRCL ou HCPN) pour traitement opérationnel, et dans quel délai moyen cette transmission s'est-elle effectuée ?

7. Combien de sanctions administratives ont été prononcées par l'ILR à l'encontre d'entités pour défaut ou retard de notification d'incident depuis l'entrée en vigueur de la loi ? Si aucune sanction n'a été prononcée, comment le Ministre explique-t-il l'absence de recours à cet outil de dissuasion ?

8. L'ILR a-t-elle procédé à des contrôles proactifs ou des exercices de simulation pour vérifier la capacité des opérateurs de services essentiels à notifier un incident dans les délais requis ?

9. L'ILR publie-t-elle un rapport annuel ou des statistiques agrégées sur les incidents notifiés, comme le prévoit le cadre européen ? Si non, le Gouvernement envisage-t-il de rendre ces données publiques afin de renforcer la transparence et la sensibilisation ?

10. Quelles sont les principales typologies d'incidents notifiés (ransomware, DDoS, compromission de données, défaillance technique) et quelles tendances se dégagent par rapport aux années précédentes ?

11. Comment la coordination entre l'ILR, le HCPN, le CIRCL et, le cas échéant, la CSSF s'organise-t-elle concrètement lors de la réception d'une notification d'incident affectant plusieurs secteurs ou ayant un impact transfrontalier ?

Mat déiwem Respekt,

CLEMENT Sven
Deputéierten