N°4332
Entrée le 27.07.2026
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Réponse commune de Monsieur le Premier ministre, Luc FRIEDEN, Ministre de l'Économie, des PME, de l'Énergie et du Tourisme, Lex DELLES et de Madame la Ministre déléguée auprès du Premier ministre, chargée des Médias et de la Connectivité, Elisabeth MARGUE, à la question parlementaire n°4332 du 26 juin 2026 de l'honorable Député Sven CLEMENT au sujet de Notification des incidents de cybersécurité (NIS1).

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.) ?**

En 2025, l'Institut en tant qu'autorité compétente NIS a reçu 27 notifications incidents d'opérateurs de services essentiels NIS sous la loi du 28 mai 2019.

- 10 incidents du secteur énergie
- 5 incidents du secteur transport
- 7 incidents du secteur santé
- 5 incidents du secteur Infrastructures numériques

En tant que point de contact unique NIS, l'ILR a reçu 6 notifications d'incidents significatifs pour les services financiers pour lesquels la CSSF était l'autorité compétente sous NIS 1.

En plus des incidents qui ont été notifiés sous la loi NIS, l'ILR a également reçu 15 notifications incidents d'opérateurs de réseaux ou de services de communications électroniques sous la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques dont 13 incidents significatifs.

En outre, plusieurs notifications préliminaires qui ont été envoyées à l'ILR, n'ont pas été suivies par une notification incident complète dû au fait que l'incident n'était pas significatif.

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 ?**

Parmi les notifications NIS 1 reçues par l'ILR en tant qu'autorité compétente, 11 ont été classifiées comme incidents « significatifs ».
L'ILR a publié des règlements sectoriels permettant aux entreprises et à l'ILR de déterminer si un incident est à considérer comme significatif.

- Règlement ILR/N21/1 du 9 juin 2021 portant définition des paramètres et modalités en relation avec la notification d'un incident ayant un impact significatif sur la fourniture d'un service numérique par les fournisseurs de services numériques à signaler à l'institut ;
- Règlement ILR/N21/2 du 4 octobre 2021 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur eau potable ;
- Règlement ILR/N22/1 du 22 février 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport – sous-secteur transport ferroviaire ;

- Règlement ILR/N22/2 du 15 juin 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport – sous-secteur transport routier ;
- Règlement ILR/N22/3 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur de l'énergie – sous-secteur gaz ;
- Règlement ILR/N22/4 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur de l'énergie - Sous-secteur électricité – NISS ;
- Règlement ILR/N22/5 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur santé ;
- Règlement ILR/N22/6 du 3 août 2022 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur infrastructure numérique ;
- Règlement ILR/N23/1 du 2 mai 2023 portant définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur transport sous-secteur transport aérien ;
- Règlement ILR/N23/3 du 20 juillet 2023 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services de communications électroniques.

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 ?

L'ILR n'établit actuellement pas de statistiques sur le délai moyen entre la survenance d'un incident et sa notification.

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) ?

Dans un premier temps, l'Institut a régulièrement émis une « demande d'information » tel qu'il était prévu par l'article 9, respectivement l'article 12 de la Loi du 28 mai 2019 « NIS ».

Généralement, les opérateurs ont été très collaboratifs, ce qui a permis d'avoir de bons échanges. Aucune sanction pour notification d'incident incomplète ou tardive a dû être émise en 2025.

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 ?

En ce qui concerne les mécanismes de détection : l'Institut peut être informé d'incidents par le biais des « clients/utilisateurs » d'un service affecté, par les médias ou par le biais d'une notification d'incident d'un opérateur affecté par un incident s'étant produit chez un autre opérateur. A ce moment, l'Institut adresse une « demande d'information » à l'opérateur concerné pour vérifier la véracité des propos et/ou d'exiger qu'une notification d'incident soit faite.

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 ?

Grâce à la plateforme SERIMA, la transmission des informations relatives à une notification d'incident se fait immédiatement au moment de la soumission d'une pré-notification.

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 ?**

Sous le régime de la Loi du 28 mai 2019 « NIS », aucune sanction pour défaut ou retard de notification d'incident n'a été prononcée par l'Institut en 2025. Ceci est principalement dû au fait que suivant la demande d'information adressée aux entités, elles se présentent très collaboratives. Souvent, le retard ou le défaut de notification est dû à une mauvaise compréhension des critères de notification applicables. Une fois cet aspect clarifié par l'Institut, les entités procèdent directement à la notification d'incident.

Toutefois, pour l'année 2026, une procédure de sanction relative à un défaut de notification est actuellement en cours.

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 ?**

L'ILR organise chaque année un exercice cyber avec différentes entités sous la supervision de l'Institut qui a comme but de simuler la capacité des opérateurs à réagir en cas d'incident ce qui inclut la capacité des opérateurs concernés de notifier des incidents à l'autorité compétente.

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 ?**

L'ILR inclut dans son rapport d'activité, disponible via le site web de l'ILR, des statistiques agrégées sur les incidents notifiés.

En tant que point de contact unique sous la loi NIS 1, l'ILR a également partagé des données agrégées au niveau européen à travers la plateforme CIRAS de l'ENISA.

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 ?**

Actuellement, l'ILR n'établit pas de statistiques sur la typologie des incidents notifiés. Cependant, au Luxembourg un grand nombre d'incidents notifiés sont dus à des défaillances techniques et non pas à des actes malicieux. Pour les actes malicieux nous pouvons voir les mêmes tendances au Luxembourg qu'en Europe.

11. **Comment la coordination entre l'ILR, le HCPN, le CIRCL et, le cas échéant, la CSSF s'organise-telle concrètement lors de la réception d'une notification d'incident affectant plusieurs secteurs ou ayant un impact transfrontalier ?**

Afin de préparer la coordination entre les différents acteurs, l'ILR a mis en place une plateforme de notification incident qui peut être utilisée par plusieurs autorités. Depuis la transposition de la directive NIS 2 en loi nationale, les incidents NIS sont automatiquement partagés avec le HCPN en tant que point de contact unique NIS et avec le CSIRT responsable de l'entité notifiant l'incident (CIRCL ou GOVCERT.LU). Le cas échéant, les CSIRT se concertent et coopèrent pour offrir un support de remédiation aux entités affectées.

En cas de réception d'une notification d'incident significatif affectant plusieurs secteurs ou ayant un impact transfrontalier, les mécanismes de gestion de crise définis par le Plan gouvernemental de gestion de crise cybernétique et numérique sont activés par des acteurs désignés, dont notamment l'ILR, la CSSF, le HCPN avec GOVCERT.LU et le CIRCL. L'impact aux niveaux national et transfrontalier de l'incident significatif est évalué par la Cellule d'Évaluation du Risque Cyber (CERC) suivant un cadre de classification d'incident. La coordination des mesures de réponse peut intervenir au niveau de la CERC ou, au besoin, peut être portée au niveau politique par l'activation d'une Cellule de Crise (CC).
En cas d'impact transfrontalier, le HCPN, dans son rôle de point de contact unique NIS, assure la transmission de la notification d'incident aux autorités compétentes des États membres de l'Union européenne impactés.

Luxembourg, le 27 juillet 2026

Le Premier ministre,

(s.) Luc FRIEDEN