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

Réponse du Premier ministre, de la Ministre de la Digitalisation et du Ministre des Affaires intérieures, à la question parlementaire n° 4991 du 22 octobre 2026 des honorables Députées Octavie Modert et Françoise Kemp.

1. **Dans quelle mesure les services numériques de l'État et des établissements publics ont-ils été exposés aux deux vulnérabilités identifiées ? Combien de systèmes ont été reconnus comme potentiellement vulnérables et quelle proportion a, à ce jour, fait l'objet de correctifs dont l'application effective a été vérifiée ? Des systèmes demeurent-ils exposés ou temporairement indisponibles dans l'attente de leur sécurisation ?**

L'État, en tant qu'entité hautement digitalisée, était mécaniquement concerné par les vulnérabilités identifiées. À cet égard, le Centre des technologies de l'information de l'État a procédé à un inventaire exhaustif, identifiant 192 systèmes concernés, dont 57 exposés sur Internet. Des mesures de mitigation rigoureuses ont été déployées pour l'ensemble des cas de figure (comprenant notamment des mises à jour correctives, des isolements temporaires, des décommissionnements ou la désactivation ciblée du composant vulnérable ou, le cas échéant, la prise de contact avec les responsables pour les systèmes hors du périmètre d'action du CTIE). Ces mesures s'appuient sur les bulletins de sécurité officiels et leurs recommandations. À ce jour, aucun des systèmes sous la responsabilité du CTIE n'est plus exposé.
Dans le cadre du suivi de la situation par la Cellule d'évaluation du risque cyber (CERC), des états des lieux complémentaires sont en cours auprès des acteurs concernés afin d'évaluer leur situation et l'état d'avancement des mesures de remédiation.

2. **Depuis le 20 octobre 2026, des tentatives d'exploitation de ces vulnérabilités ou des incidents de sécurité y afférents ont-ils été constatés ou portés à la connaissance des autorités compétentes au Luxembourg ? Le cas échéant, des compromissions effectives de systèmes ou de données ont-elles pu être établies ?**

À ce jour, aucun incident ni aucune tentative d'exploitation avérée en relation avec ces vulnérabilités n'ont été signalés au CTIE. De son côté, le GOVCERT n'a constaté aucune tentative d'exploitation des vulnérabilités. Par ailleurs, l'ILR n'a reçu aucune notification d'incident y afférente.

3. **De nombreuses communes et syndicats intercommunaux confient l'hébergement et la maintenance de leurs plateformes numériques à des prestataires externes. Comment le Gouvernement entend-il accompagner ces collectivités dans la vérification de la sécurisation effective de leurs systèmes, notamment lorsqu'elles ne disposent pas de compétences informatiques propres ? Dans quelle mesure les obligations relatives à la sécurité des prestataires, prévues par la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (NIS2), sont-elles mises en œuvre dans le secteur communal ?**

Conformément aux dispositions de la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, il revient aux communes de s'assurer que leurs services informatiques bénéficient d'un certain niveau de cybersécurité. Quant tenu de la complexité de la matière, le LHC et le « Computer Incident Response Center Luxembourg » (CIRCL) opéré par le LHC, ont pour objectif de soutenir les communes et les sociétés privées dans le but d'accroitre le niveau de qualité et de sécurité

de leurs systèmes et réseaux d'information, sans pour autant les décharger de leurs responsabilités et sans faire une concurrence déloyale aux prestataires de services cybersécurité privés. Toutefois, le LHC offre des services et outils (open-source) de sensibilisation, de gouvernance et de sécurité (notamment dans le domaine de la gestion de vulnérabilités), il entretient une newsletter avec des recommandations, organise régulièrement des séances d'informations et publie des recommandations techniques détaillées si ceci est nécessaire.

En parallèle, le ministère de l'Économie a lancé début 2026 un « package PME cyber » qui adresse spécifiquement les besoins des PME en termes de conseils et d'implémentations d'outils liés à la cybersécurité fournis par des sociétés luxembourgeoises. Pour des raisons d'aides d'État ni les communes, ni les syndicats ne sont éligibles pour ces aides.

Le ministère de l'Économie, en étroite collaboration avec le LHC, a mis en place la « cybersecurity factory » pour promouvoir le développement d'outils de cybersécurité accessibles aux communes et PME. Deux appels à projets LU-CID ont déjà été lancés avec succès pour faire développer des solutions open source.

Les communes doivent, tout comme toute société privée, elles-mêmes procéder à la mise en place, gestion et maintenance des services ou produits informatiques, en fonction de leurs risques, avec leurs propres ressources, ou recourir à des prestataires externes. Ces derniers, qui peuvent être des acteurs publics (Etat, Syndicat intercommunal de gestion informatique) ou privées, sont alors tenus, dans le cadre de leur prestation de service, d'informer leurs clients sur les éventuelles vulnérabilités rencontrées et des mesures à mettre en place.

Pour ce qui concerne les outils mis à disposition des communes par l'Etat, à savoir les services « Vote » et « otx », ils ont été, comme d'autres sites internet, mis préventivement hors service jusqu'à ce que leur niveau de sécurité ait pu être à nouveau assuré.

4. **Quelles mesures permettent d'assurer la continuité des services publics essentiels lorsqu'une plateforme numérique doit être temporairement suspendue pour des raisons de sécurité ? Des solutions alternatives sont-elles prévues pour permettre aux citoyens et aux entreprises d'accomplir leurs démarches administratives, notamment lorsqu'ils sont soumis à des délais légaux ?**

En présence d'un risque élevé affectant des systèmes essentiels, l'adoption d'une mesure d'isolation (partielle ou complète) constitue une réponse proportionnée, dont la mise en œuvre dépend de multiples facteurs techniques et opérationnels.
Concernant des démarches en ligne soumises à des délais légaux, les conditions générales d'utilisation de la plateforme MyGuichet.lu disposent expressément en leur article 10 que :« L'État assurera au mieux une disponibilité maximale du site Guichet.lu. Toutefois, sa responsabilité ne saurait être retenue en cas d'indisponibilité momentanée ou totale du site Guichet.lu. »
Néanmoins, en cas d'indisponibilité grave et prolongée empêchant l'accomplissement des formalités requises, une application bienveillante du cadre légal peut entrer en ligne de compte, la jurisprudence administrative et les principes généraux du droit reconnaissant, le cas échéant, l'existence d'un cas de force majeure susceptible de prémunir le citoyen contre la déchéance de ses droits liés au non-respect d'un délai.

5. **Au-delà de l'application des correctifs, quelles procédures permettent de vérifier, avant la remise en service des plateformes concernées, qu'aucune compromission n'est intervenue et que l'intégrité des systèmes et des données est préservée ?**

Préalablement à toute remise en service des plateformes concernées dans le périmètre d'action du CTIE, une procédure rigoureuse de vérification est menée. Celle-ci tient compte des informations et recommandations des bulletins de sécurité officiels, et inclut le cas échéant la recherche et la surveillance d'indicateurs de compromission au sein des systèmes impactés et des données issues des systèmes de centralisation des traces.

Luxembourg, le 29 octobre 2026

Le Premier ministre,

(s.) Luc FRIEDEN