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

Réponse du Premier ministre et du ministre de l'Économie à la question parlementaire N° 4914 du 13 octobre 2026 de l'honorable Député Ben POLIDORI au sujet de la cyberattaque frigos dans les supermarchés.

1. **Des magasins au Luxembourg sont-ils également concernés ? Si oui, combien ?**

Le Gouvernement ne dispose d'aucune information sur le nombre de magasins concernés au Luxembourg. Toutefois, une déclaration d'incident a été transmise à l'Institut luxembourgeois de régulation via la plateforme SERIMA par un grand magasin.

2. **Le Gouvernement a-t-il contacté les commerces pour les avertir de la faille de sécurité des modèles de frigos concernés ?**

Le « Computer Incident Response Center Luxembourg » (CIRCL) a procédé de manière proactive à l'analyse des plages d'adresses IP luxembourgeoises. Il a ensuite envoyé des notifications relatives aux vulnérabilités détectées aux adresses de contact « abuse » associées aux adresses IP concernées.

Le CIRCL a également publié le document TR-101 Security Recommendations for Industrial, Operational Technology (OT) and Internet of Things (IoT) Devices | CIRCL[1], qui formule des recommandations pour la bonne gestion de ces équipements. Par ailleurs, il a proposé aux entités luxembourgeoises qui l'ont contacté de réaliser un scan des plages d'adresses IP susceptibles d'héberger des systèmes vulnérables.

3. **Quelles réflexions sont menées sur la prévention des usages massifs de l'IA à des fins de manipulation de l'information et de protection des processus démocratiques ?**

En matière de préparation et de gestion des crises cyber, le Gouvernement s'appuie sur le dispositif national coordonné par le Haut-Commissariat à la Protection nationale (HCPN), qui exerce les fonctions d'autorité nationale de gestion des crises cyber au sens de la directive NIS2.
Le Plan gouvernemental de gestion de crise cybernétique et numérique prévoit des mécanismes permanents de préparation, d'évaluation et de qualification des incidents et menaces cyber majeurs ainsi que, lorsque la situation l'exige, l'activation des structures nationales de coordination et de gestion de crise.
Ces mécanismes permettent notamment de prendre en compte les situations dans lesquelles une cyberattaque affecterait plusieurs acteurs de la chaîne d'approvisionnement alimentaire ou provoquerait des perturbations significatives de fonctions essentielles, notamment dans les domaines de la production, du stockage, du transport ou de la distribution des denrées alimentaires.

En cas de crise majeure, la Cellule de crise assure le pilotage stratégique et les arbitrages nécessaires à la préservation et au rétablissement des services essentiels, tandis que la Cellule opérationnelle cyber (PCO-C) coordonne la gestion opérationnelle de la composante cybernétique ou numérique, en concertation avec les autorités sectorielles, les acteurs concernés et les capacités nationales de réponse aux incidents.

[1] https://new.circl.lu/pub/tr-101/

Cette organisation permet d'articuler la gestion technique des incidents cyber avec la continuité des activités essentielles et, le cas échéant, de prioriser les capacités nationales de réponse en fonction de la gravité des impacts et des besoins de la population.

Sur initiative du Premier ministre, le Comité interministériel de coordination en matière de cyber prévention et de cybersécurité (CIC-CPCS) a lancé en date du 19 octobre des travaux dédiés aux risques désormais avérés émanant de certains agents d'I.A. pour la cybersécurité (*illustrée par divers récents incidents tel que notamment celui chez HuggingFace de OpenAI*), prenant en compte l'accélération des progrès réalisés dans le développement de nouveaux agents de plus en plus autonomes, et considérant les menaces potentielles dans le domaine de la cybersécurité pouvant toucher des infrastructures critiques, voire affecter la stabilité de nos sociétés, notre économie ainsi que notre démocratie. L'objectif de ces travaux est de créer une proposition d'approche pour gérer les risques et contrer menaces venant émanant de certains « *frontier A.I. models* » (*découverte de vulnérabilités, accélération des attaques…*)

Luxembourg, le 9 novembre 2026

Le Premier ministre,

(s.) Luc FRIEDEN