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° 4907 du 13 octobre 2026 de l'honorable Député Marc Goergen au sujet de la cyberattaque frigos dans les supermarchés.

1. **Huet d'Regierung Kenntnis dovun, ob zu Lëtzebuerg Supermarchéen, Liewensmëttelbetriber oder aner Acteuren aus der Liewensmëttelketten änlech vernetzt Frigo- respektiv Killsystemer benotzen, wéi déi, déi a Frankräich viséiert goufen?**

De Computer Incident Response Center Luxembourg (CIRCL) huet iwwert seng Europäesch Partner Informatioune kritt fir am Internet vulnerabel Frigo- respektif Killsystemer ze fannen. De CIRCL huet mat dësen Informatiounen am LU Internet Domain IP Adresse fonnt déi dëse Kriteren entspriechen. De CIRCL huet dunn de respektiven Internet Service Provider proaktif informéiert an den ISP gebieden d'Clienten hannert dësen IP-Adressen iwwert dës Schwaachstellen ze informéieren.

2. **Huet d'Regierung Kenntnis doriwwer, ob och zu Lëtzebuerg änlech Cyberugréff an der Vergaangenheet lancéiert goufen?**

Och wann et Cyberugréffer op um Internet connectéiert Computeren, Serveren, oder aner Geräter (ewéi z.B. Frigoen) reegelméisseg gëtt, huet d'Regierung keng Kenntnisser dass et zu Lëtzebuerg och sou Ugréffer op Killsystemer gi wier.

3. **Wéi eng Moossnamen goufen ëmgesat, fir eist Land virun esou Cyberugréff ze verhënneren?**

Grondsätzlech sinn Entitéiten déi informatesch Systemer oder Internet connectéiert Infrastrukture bedreiwe selwer an der Responsabilitéit fir hir Systemer um aktuellste Sécherheetsstand ze halen an sech vun hire Fournisseuren déi néideg Garantië kontraktuell ze assuréieren. Dëst fir, am Fall wou Schwaachstellen an der Software fonnt ginn, dës Fournisseuren déi néideg Sécherheetsupdatë méiglechst séier zur Verfügung stellen. Donieft mussen déi Entitéiten sech organisatoresch ëmstelle fir dës Updaten och esou séier wéi méiglech kënnen an hiren Infrastrukturen anzespillen, dës natierlech ënnert der Berücksichtegung vum operationellen Impakt déi Maintenancë vun ICT Systemer mat sech bréngen.

D'Gesetz vum 5. Mee 2026 iwwert d'Cybersécherheet (Loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité ; « NIS 2 Gesetz ») hëllt an dem Sënn d'Direktiounsorganer vun de reguléierten Entitéiten an d'Responsabilitéit.

Donieft obligéiert d'NIS2 Gesetz essenziell a wichteg Entitéiten eng reegelméisseg Analys vun hire Cyberrisiken ze maachen an entspriechend Moossnamen ze huelen, dëst ënnert der Supervisioun vun der kompetenter Autoritéit fir de Secteur. Am Fall vum Secteur alimentaire ass den ILR zoustänneg.

Op Basis vun der Evaluatioun vun dëse Risikoanalysen, huet d'kompetent Autoritéit och d'Méiglechkeet de reguléierten Entitéite Moossnamen ze recommandéiere fir dës Risike besser ze kontrolléieren. An engem zweete Schrëtt kann d'kompetent Autoritéit och Moosnamen obligéieren.

Weider garantéiert dëst Gesetz de reguléierten Entitéiten eng Rei vu Servicer vun deem fir de Secteur zoustännegen CSIRT. Fir de Secteur alimentaire ass de CIRCL zoustänneg. D'NIS 2 Gesetz bréngt zousätzlech de Support vun engem nationale Coordinateur fir eng coordonéiert Divulgatioun vu Schwaachstellen („Coordinated Vulnerability Disclosure"). Dës Moossnam hëlleft de Suivi vu Faillen a Softwarë besser ze suivéieren a fir déi méiglech impaktéiert Entitéite schnellstméiglech ze informéiere fir dass si hir Systemer kënnen updaten. De Suivi gëtt weider ënnerstëtzt duerch eng Europäesch Zentralisatioun vun ëffentlechen Informatiounen zu Schwaachstellen, dëst an enger Datebank déi vun der Agence fir d'Cybersécherheet vun der Europäescher Unioun (ENISA) geréiert gëtt. Dës ëffentlech Datebank steet alle Bedreiwer a Fournisseure vun ICT-Infrastrukturen a Servicer zur Verfügung.

Nieft dem NIS 2 Gesetz ass och den Europäesche „Cyber Resilience Act" relevant (Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques [...]). Dëst EU Reglement stellt Cybersécherheetsufuerderungen un all Produit mat digitalen Elementer, also och u vernetzt technesch Systemer wéi Frigo- a Killsystemer. D'Hiersteller mussen hir Produite sécher konzipéieren, Schwaachstellen iwwert de ganze Liewenszyklus geréieren, an aktiv exploitéiert Faille mellen. Dës Verpflichtungen trieden no an no bis 2027 a Kraaft.

Lëtzebuerg, den 9. November 2026

De Premierminister,

(s.) Luc FRIEDEN