



Réponse de la Ministre de la Digitalisation et du Premier ministre à la question parlementaire n° 1766 du 13 janvier 2025 de Monsieur le Député Laurent Mosar.

Le CTIE s'appuie sur différents systèmes de sécurité pour protéger l'infrastructure informatique de l'État. Ces systèmes fonctionnent de manière complémentaire pour garantir une protection de haut niveau. Les équipes du CTIE revoient de manière continue les configurations de ces systèmes afin de les adapter aux circonstances actuelles. Les connaissances acquises durant les incidents précédents (dont celui de mars 2024, mais également d'octobre 2024) permettent davantage d'optimiser les algorithmes de protection. Il reste à noter que les systèmes de sécurité du CTIE interceptent chaque jour du trafic malveillant adressé au réseau du CTIE.

Le CTIE investit aussi régulièrement dans l'acquisition de nouveaux systèmes de sécurité afin de profiter de nouvelles technologies plus performantes et state-of-the art pour contrer les attaques cyber qui évoluent également en termes de technologie, étant donné que les attaquants profitent aussi de leur côté du progrès technologique.

Pour des raisons de sécurité, le CTIE ne communique pas le détail technique des mesures de protection en place.

Les sites web gouvernementaux hébergés par le CTIE ont été touchés par l'attaque DDoS le vendredi 10 janvier de 13h05 à 14h55 et ont été inaccessibles durant ce laps de temps. En parallèle, en raison de perturbations chez la société LuxTrust, il n'a pas été possible de se connecter avec un produit Luxtrust aux services en ligne proposés par le CTIE, aux citoyens et aux applications internes de l'Etat, qui nécessitent une authentification forte, jusque peu après 18h00. Une connexion avec GouVID sur MyGuichet.lu et l'utilisation de l'application MyGuichet.lu, pour tous les utilisateurs qui ont lié l'application à leur espace privé MyGuichet.lu, était à nouveau possible à partir de 14h55. Toutefois, les agents étatiques ont pu se connecter aux applications internes grâce à un produit alternatif basé sur un One-Time-Password qui fonctionne de manière similaire au Token LuxTrust.

Le CTIE a la mission de protéger l'infrastructure informatique étatique. Dans le cadre de cette mission, il dispose de différents outils de gestion des crises pour coordonner les actions de ses différentes équipes qui interviennent dans le cadre d'une attaque cyber. Les procédures et outils sont adaptées grâce aux connaissances acquises durant les attaques précédentes afin de les rendre davantage efficaces.

Au niveau national, le plan d'intervention d'urgence "PIU Cyber" définit l'action du gouvernement en cas de faille technique ou d'attaque d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé.

Le PIU Cyber définit notamment les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises.



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

Luxembourg, le 12/02/2025.

La Ministre de la Digitalisation

(s.) Stéphanie Obertin