N°99
Entrée le 16.01.2024
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires intérieures

Réponse du Ministre des Affaires intérieures, Léon Gloden, de Madame la Ministre de la Justice et Ministre déléguée auprès du Premier ministre, chargée des Médias et de la Connectivité, Elisabeth Margue, et de Monsieur le Ministre de l'Economie, des PME, de l'Energie et du Tourisme, Lex Delles, à la question parlementaire n° 99 de l'honorable Député Yves Cruchten au sujet de l'augmentation inquiétante des attaques d'hameçonnage.

Question 1

Les cyberattaques et la cybercriminalité augmentent sensiblement en nombre et en sophistication au Luxembourg ainsi que dans toute l'Europe, avec une tendance qui devrait encore d'avantage s'accentuer à l'avenir.

Les attaques d'hameçonnage sont une forme d'escroquerie qui vise à voler les informations personnelles des utilisateurs. En ce qui concerne le nombre d'affaires en matière d'hameçonnage ou phishing au Luxembourg, celui-ci est passé de 28 affaires en 2020 à 1310 affaires en 2023.

Les données ou statistiques en rapport avec la cybersécurité et les attaques informatiques, sont publiées dans le rapport que l'Agence nationale de cybersécurité au service de l'économie luxembourgeoise et des communes, devenue la Luxembourg House of Cybersecurity (LHC), a récemment publié « A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME Sector » (https://observatory.nc3.lu/market-intelligence-library/report-2023/). De plus, le CIRCL et NC3 publient régulièrement des statistiques par rapport aux menaces, dont le phishing, sur leurs sites internet (https://circl.lu/opendata/statistics/ et https://observatory.nc3.lu/observatory-bulletin/2023/2/).

Aussi, la Police grand-ducale publie chaque année les chiffres de la délinquance.

Question 2

La Police grand-ducale ne dispose ni de statistiques spécifiques ni d'estimations des dommages causés en lien avec ce phénomène spécifique.

Question 3

A l'heure actuelle aucune condamnation n'a été prononcée pour une affaire de phishing.

Question 4

Au sein de la Police grand-ducale chaque policier peut prendre en charge des plaintes dans le cadre d'une affaire de phishing.

Au sein des parquets Diekirch et Luxembourg, une équipe de 5 personnes au total est en charge de ces dossiers.

Question 5

Lorsque des liens internationaux entres diverses séries de phishing sont constatés, ceux-ci sont évidemment discutés, notamment au sein d'institutions européennes telles qu'Europol.

Question 6

La Police grand-ducale informe sur son site Internet et à travers les médias sur le sujet de l'hameçonnage et dirige les visiteurs via un lien sur le site internet BeeSecure avec des informations supplémentaires.

Questions 7 et 8

Face à l'augmentation des appels frauduleux ayant recours à des numéros géographiques luxembourgeois en provenance de l'étranger constatée par les opérateurs de communications électroniques ces derniers temps, l'ILR a adopté le 8 janvier 2024 le Règlement ILR/T24/1 relatif au blocage des appels provenant de numéros géographiques au départ d'un pays autre que le Grand-Duché de Luxembourg. Afin de protéger les clients finaux d'appels frauduleux, les opérateurs peuvent désormais bloquer les appels provenant de numéros géographiques luxembourgeois au départ d'un pays autre que le Grand-Duché de Luxembourg, s'ils disposent d'éléments suffisants qui leur permettent de déduire que ceux-ci poursuivent des objectifs frauduleux. En cas de blocage injustifié d'un numéro, une procédure de recours est prévue.

Question 9

Les efforts et les investissements du gouvernement en matière de cybersécurité de ces dernières années renforcent la protection des citoyens et des entreprises face aux attaques informatiques de tout type. Le ministère de l'Économie a commencé à investir dans la cybersécurité il y a 20 ans. C'est ainsi qu'un secteur aux activités diversifiées autour de la cybersécurité a progressivement vu le jour et qu'est née l'Agence nationale de cybersécurité au service de l'économie luxembourgeoise et des communes, initialement connue sous le nom Securitymadein.lu et désormais nommée Luxembourg House of Cybersecurity (LHC). Ceci s'inscrit dans l'exécution du programme gouvernemental dans lequel le gouvernement s'engage à renforcer « *les moyens techniques et humains pour lutter efficacement contre la cybercriminalité* » (dans le chapitre digitalisation) et « *lancera un programme SME Package Cyber Security pour accompagner les petites et moyennes entreprises (PME) dans la mise en place de mesures de sécurité informatique* », comme inscrit sous le chapitre Cybersécurité, qui annonce également la création du « *Luxembourg House of Cybersecurity* » pour récolter *« les données concernant les menaces et vulnérabilités* (…)». Le gouvernement a également inscrit dans son programme sous le chapitre Renforcement de la sécurité d'approvisionnement qu'il allait fournir « *un effort concerté au niveau des ministères concernés, du Haut-commissariat à la protection nationale, des gestionnaires de réseau et d'autres acteurs concernés du secteur. Une attention particulière sera accordée à la cybersécurité, à l'interdépendance avec d'autres secteurs (dont par exemple les télécommunications) et aux exercices de crise* ».

La LHC propose, entre autres, des lieux d'accueil pour les citoyens (initiative BEE SECURE), pour les acteurs de la recherche et de l'innovation (Digital Innovation Hub, Digital Learning Hub), ainsi que pour les start-up dans le domaine de la cybersécurité. La LHC consolide ses activités sur 2 centres d'expertise :

- CIRCL (Computer Incident Response Centre Luxembourg), pour la gestion d'incidents et la promotion d'échanges et de renseignements sur la menace cyber.

- NC3 (National Cybersecurity Competence Centre), qui représente notamment le Luxembourg en tant que centre national de coordination en au sein du réseau du Centre européen de compétences en matière de cybersécurité.

En ce qui concerne les entités de poursuite nationales, le gouvernement leur mettra à disposition les ressources personnelles et matérielles requises pour lutter contre la cybercriminalité.

Enfin, la Police continue de sensibiliser la population aux attaques et arnaques via son site internet et les médias.

Question 10

La « Cybersecurity Week Luxembourg » est importante en vue de la sensibilisation. Celle-ci se déroule tous les ans pendant le mois dédié à la cybersécurité au niveau européen et des événements de sensibilisation sont organisés. L'écosystème public de la cybersécurité a publié en 2021 un outil anti-spam et anti-phishing important pour combattre le hameçonnage nommé SPAMBEE (https://www.bee-secure.lu/fr/tool/outil-anti-spam-et-anti-phishing/) ainsi que des conseils pratiques (https://www.bee-secure.lu/wp-content/uploads/2023/09/153_risques-sur-internet_ua.pdf ou encore https://police.public.lu/fr/prevention/dangers-sur-internet/phishing.html).

De plus, la Police grand-ducale ainsi que BeeSecure lancent régulièrement des campagnes de sensibilisation sur le sujet du phishing.

Luxembourg, le 16 janvier 2024
Le Ministre des Affaires intérieures
(s.) Léon Gloden